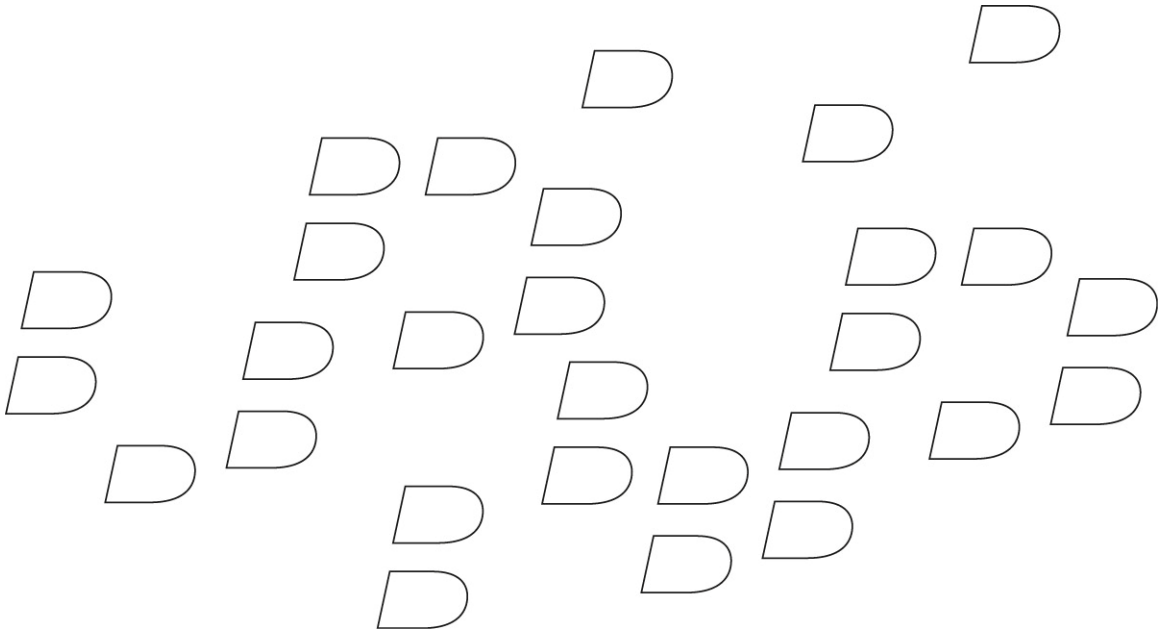


BlackBerry Enterprise Solution Security

Version 4.1.0

Technical Overview

© 2006 Research In Motion Limited. All rights reserved.

Contents

Wireless security 4
BlackBerry Enterprise Solution security 4
New security features 6
BlackBerry encryption keys 6
Master encryption key 6
Message key 9
Content protection key 10
Grand master key 11
BlackBerry symmetric key encryption algorithms 12
Standard BlackBerry message encryption 12
BlackBerry wireless messaging security 14
Receiving an email message on the BlackBerry device 14
Sending an email message from the BlackBerry device 14
Message attachment viewing security 15
PIN messaging 15
SMS and MMS messaging 16
Controlling unsecured messaging 16
Extending BlackBerry device messaging security 16
PGP Support Package 16
PGP encryption 17
S/MIME Support Package 18
S/MIME encryption 19
Decrypting and reading messages on the BlackBerry device using Lotus Notes API 7.0 20
Protecting stored data 21
Protecting stored messages on the messaging server 21
IT policy signing and storage on the BlackBerry device 22
Application password encryption and storage on the BlackBerry device 22
Protected storage of user data on a locked BlackBerry device 22
Protected storage of master encryption keys on a locked BlackBerry device 23
Protected storage of master encryption keys on a BlackBerry device during a reset 24
Cleaning the BlackBerry device memory 24
BlackBerry architecture component security 25
BlackBerry Infrastructure 26
BlackBerry Enterprise Server 26

© 2006 Research In Motion Limited. All rights reserved.

Messaging server 26
BlackBerry configuration database 26
BlackBerry MDS Services databases 28
Protecting the BlackBerry Infrastructure connections 28
SRP authentication 29
BlackBerry Router protocol authentication 30
Wireless enterprise activation authentication 31
TCP/IP connection 32
Messaging server to desktop email program connection 33
BlackBerry Mobile Data System connections 34
WAP gateway connections 35
Authenticating a user 35
Authenticating a user to a BlackBerry device using a password 35
Authenticating a user using a smart card 35
Controlling BlackBerry devices 37
Controlling BlackBerry device behaviour using IT policy rules 37
Enforcing device and desktop security 38
Controlling BlackBerry device access to the BlackBerry Enterprise Server 39
Protecting Bluetooth connections on BlackBerry devices 39
Protecting the BlackBerry device against malware 40
Protecting lost, stolen, or replaced BlackBerry devices 42
Erasing data from BlackBerry device memory and making the BlackBerry device unavailable 43
Unbinding the smart card from the BlackBerry device 43
Related resources 44
Appendix A: RIM Cryptographic Application Programming Interface 46
Cryptographic functionality that the RIM Crypto API provides 46
Appendix B: TLS and WTLS standards that the RIM Crypto API supports 48
Key establishment algorithm cipher suites that the RIM Crypto API supports 48
Symmetric algorithms that the RIM Crypto API supports 49
Hash algorithms that the RIM Crypto API supports 49
Appendix C: Previous version of wired master encryption key generation 50
Previous version of wired master encryption key generation process 50
Appendix D: BlackBerry device wipe process 51
Appendix E: Ephemeral AES encryption key derivation process 53

© 2006 Research In Motion Limited. All rights reserved.

This document describes the security features of the BlackBerry® Enterprise Solution and provides an overview of the BlackBerry security architecture.

This document describes the security features that BlackBerry Enterprise Server version 4.1 or later, BlackBerry Desktop Software version 4.1 or later, and BlackBerry Device Software version 4.1 or later support, unless otherwise stated. See the documentation for earlier versions of the BlackBerry Enterprise Server, BlackBerry Desktop Software, and BlackBerry Device Software to determine if a feature is supported in that earlier software version.

See the *BlackBerry Enterprise Solution Security Acronym Glossary* for the full terms substituted by the acronyms in this document.

Wireless security

Many companies are realizing significant return on investments and productivity gains by extending their enterprise information to mobile employees. With an increased demand for mobile content and the threat of information theft, companies have concerns about addressing security needs and requirements when evaluating wireless solutions. Without an effective security model, your company might expose sensitive corporate data, with financial and legal implications.

With the advent of powerful new personal devices such as mobile phones and personal digital assistants that can access and store sensitive corporate data, controlling access to these devices is an important issue. Leaving devices with remote access to sensitive data accessible to potentially malicious users could be dangerous.

The BlackBerry Enterprise Solution (consisting of a BlackBerry device, BlackBerry Device Software, BlackBerry Desktop Software, and the BlackBerry Enterprise Server software) is designed to protect your corporation from data loss or alteration in the event of

- malicious interception of data on the corporate network, while a user is sending and receiving messages and accessing corporate data wirelessly using the BlackBerry device
- an attack intended to steal corporate data, using malicious application code (for example, a virus)
- theft of the BlackBerry device
- identity theft

BlackBerry Enterprise Solution security

The BlackBerry Enterprise Solution implementation of *symmetric key cryptography* is designed to provide confidentiality, integrity, and authenticity implicitly.

Concept	Description	BlackBerry Enterprise Solution implementation
confidentiality	permits only the intended message recipient to view the contents of a message	• Use encryption, which is data scrambling based on a secret key, to make sure that only the intended recipient can view the contents of the message.
integrity	enables a message recipient to detect if a third-party altered the message data in transit between the message sender and the message recipient	• Protect each message that the BlackBerry device sends with one or more message keys comprised of random information, which is designed to prevent third-party decryption or alteration of the message data. • Enable only the BlackBerry Enterprise Server and the BlackBerry device to know the value of the master encryption key, recognize the format of the decrypted and decompressed message, and automatically reject a message either one receives that is encrypted with the wrong master encryption key and therefore does not produce the required message format upon decryption.

Concept	Description	BlackBerry Enterprise Solution implementation
authenticity	enables the message recipient to identify and trust the identity of the message sender	• Require that the BlackBerry device authenticate itself to the BlackBerry Enterprise Server to prove that it knows the master encryption key before the BlackBerry Enterprise Server can exchange the unique master encryption key with, and send data to the BlackBerry device.

The BlackBerry Enterprise Solution is designed so that data remains encrypted (in other words, it is not decrypted) at all points between the BlackBerry device and the BlackBerry Enterprise Server. Only the BlackBerry Enterprise Server and the BlackBerry device have access to the data that they send between them. Thus, third-parties, including service providers, cannot access potentially sensitive company information in a decrypted format.

Message failure occurs automatically if the BlackBerry device cannot recognize the message format produced by the BlackBerry Enterprise Server decryption process, or if the BlackBerry Enterprise Server receives a message encrypted with the wrong master encryption key. If message failure occurs, the BlackBerry device prompts the user to generate a new master encryption key (required).

BlackBerry Enterprise Solution feature	Description
protect data	• Encrypt data traffic in transit between the BlackBerry Enterprise Server and the BlackBerry device. • Encrypt data traffic in transit between your messaging and collaboration server and a user's desktop email program. • Use secure protocols to connect the BlackBerry Enterprise Server to the BlackBerry Infrastructure. • Encrypt data on the BlackBerry device. • Encrypt data in the BlackBerry configuration database. • Authenticate a user to the BlackBerry device using a smart card with a password or passphrase.
protect encryption keys	• Encrypt encryption keys on the BlackBerry device.
control BlackBerry device connections	• Control which BlackBerry devices can connect to the BlackBerry Enterprise Server. • Control Bluetooth® connections to and from the BlackBerry device. • Control BlackBerry Smart Card Reader connections.
control BlackBerry device and BlackBerry Desktop Software functionality	• Send wireless commands to turn on and turn off BlackBerry device functionality, delete information from BlackBerry devices, and lock BlackBerry devices. • Send IT policies to customize security settings for a user or a group on a BlackBerry Enterprise Server. • Enforce BlackBerry device and BlackBerry Smart Card Reader passwords.

New security features

Feature	Software versions supported	Description
protect master encryption keys on the BlackBerry device	• BlackBerry Enterprise Server version 4.1 (all platforms) • Java™ based BlackBerry devices that are running BlackBerry device software version 4.1 or later	Encrypt the master encryption keys stored on the BlackBerry device in flash memory using 256-bit AES.
support smart cards with the BlackBerry Smart Card Reader	• BlackBerry Smart Card Reader version 1.0 • Bluetooth-enabled BlackBerry devices that support Bluetooth specification version 1.1 and are running BlackBerry device software version 4.0.0 or later • BlackBerry Enterprise Server version 4.0.2 (with the S/MIME IT Policy template imported) or BlackBerry Enterprise Server version 4.0.3 or later (all platforms)	Use the BlackBerry Smart Card Reader accessory to enable a user to authenticate and communicate wirelessly with a supported Bluetooth-enabled BlackBerry device. See the *BlackBerry Smart Card Reader Security White Paper* for more information.
send and receive PGP® messages	• PGP Support Package version 4.1 • BlackBerry Enterprise Server version 4.0 Service Pack 2 or later for Microsoft Exchange • BlackBerry Enterprise Server version 4.1 for IBM Lotus Domino • Java based BlackBerry devices that are running BlackBerry device software version 4.1 or later	Permit a user who is already sending and receiving PGP protected messages using their desktop email program to send and receive PGP protected messages, and decrypt and read received PGP protected messages using their BlackBerry device. See the *PGP Support Package White Paper* for more information.
decrypt and read IBM® Lotus Notes-encrypted and S/MIME-encrypted messages	• BlackBerry Enterprise Server version 4.1 for IBM Lotus Domino • Java based BlackBerry devices that are running BlackBerry device software version 4.1 or later	Use Lotus Notes® API 7.0 to automatically decrypt messages on the BlackBerry device that the sender has encrypted using either IBM Lotus Notes or S/MIME encryption.

BlackBerry encryption keys

By default, the BlackBerry Enterprise Solution generates the *master encryption key* and *message key* that the BlackBerry Enterprise Server and BlackBerry devices use to encrypt and decrypt all data traffic between them.

You can also enable the BlackBerry device to generate and use the *content protection key* to encrypt user data while the BlackBerry device is locked, and generate and use the *grand master key* to encrypt the master encryption key while the BlackBerry device is locked.

Master encryption key

The master encryption key is unique to the BlackBerry device. To send and receive messages, all master encryption keys stored on the BlackBerry Enterprise Server and the BlackBerry device must match. If the stored keys do not match, the BlackBerry device or the BlackBerry Enterprise Server cannot decrypt and must therefore discard messages that they receive.

Master encryption key storage

The BlackBerry configuration database, the messaging server, and the BlackBerry device flash memory store encryption keys, including the current BlackBerry device master encryption key (in other words, the master encryption key that the BlackBerry device currently uses to encrypt and decrypt message keys).

Messaging server platform	Messaging server storage location	BlackBerry device storage location	BlackBerry Enterprise Server storage location
IBM Lotus® Domino® server	the BlackBerry profiles database	a key store database in flash memory	the BlackBerry configuration database
Microsoft® Exchange server	the desktop email program user mailbox	a key store database in flash memory	the BlackBerry configuration database
Novell® GroupWise® server	not stored	key store database in flash memory	the BlackBerry configuration database

It is critical to protect the BlackBerry configuration database and the platform-specific master encryption key storage location on the messaging server. See "Messaging server to desktop email program connection" on page 33 and "Protecting the BlackBerry configuration database" on page 26 for information.

The BlackBerry configuration database, the messaging server, and the BlackBerry device flash memory can also retain previous and pending master encryption keys.

Key state	Description
previous key(s)	The master encryption key(s) that the BlackBerry device used before the current key was generated. The BlackBerry device stores multiple previous keys in flash memory for 7 days, the maximum amount of time that the BlackBerry Enterprise Server queues a pending message for delivery, in case the user creates a new key on the BlackBerry device multiple times while messages are still queued on the BlackBerry Enterprise Server. The messaging server and the BlackBerry configuration database store only the most recent previous key.
pending key	The master encryption key that you generate in the BlackBerry Manager or the user generates on the BlackBerry device to replace the current master encryption key. Only the messaging server and the BlackBerry configuration database store the pending key. The BlackBerry Desktop Software sends the pending key to the BlackBerry device when the user connects the BlackBerry device to the desktop computer. The current key then becomes the new previous key, and the pending key becomes the new current key.

Master encryption key generation

Both you and a user can generate and regenerate master encryption keys.

Key generation method	Initial key generation	Key regeneration
desktop-based (wired)	When a user connects the BlackBerry device to the desktop computer for the first time, the BlackBerry Desktop Software creates the master encryption key and sends it to the BlackBerry device and the messaging server.	When the user subsequently connects the BlackBerry device to the desktop computer, the user can initiate regeneration of the master encryption key. The BlackBerry Desktop Software creates the master encryption key and sends it to the BlackBerry device and the messaging server.

Key generation method	Initial key generation	Key regeneration
wireless	Wireless enterprise activation permits a user to remotely activate a BlackBerry device on the BlackBerry Enterprise Server without a physical network connection. During the wireless enterprise activation, the BlackBerry Enterprise Server and the BlackBerry device negotiate to select the strongest algorithm that they both support and use that algorithm to generate the master encryption key. **Note**: See "Wireless enterprise activation authentication" on page 31 for more information.	On the BlackBerry device, a user can request a new master encryption key. The BlackBerry device sends the key regeneration request to the BlackBerry Enterprise Server wirelessly. In the BlackBerry Manager, you can initiate regeneration of a master encryption key for a BlackBerry device.

Desktop-based master encryption key generation process

In BlackBerry Desktop Software version 4.0 or later, the master encryption key generation function uses the current time as the seed for the C language srand function. The master encryption key generation function then gathers entropy (randomness) using the following process:

1. When prompted by the BlackBerry Desktop Software, the user moves the mouse. The ARC4 encryption algorithm examines the lowest 12 bits of the x and y axes of the new mouse location. If the bits are different from the previous sample, the BlackBerry Desktop Software stores them, generating 3 bytes of randomness. If the bits are the same as the previous sample, no sample is taken.
2. The ARC4 encryption algorithm sleeps for a random interval between 50 and 150 milliseconds, and then samples again.
3. The ARC4 encryption algorithm loops until it gathers 384 bytes.
4. The BlackBerry Desktop Software retrieves 384 bytes of randomness from the MSCAPI, for a total of 768 bytes.
5. The BlackBerry Desktop Software hashes the 384 bytes of randomness from the ARC4 encryption algorithm and the 384 bytes of randomness from the MSCAPI with SHA512 to produce 512 bits of data. The BlackBerry Desktop Software frees the memory associated with the unused bits.
6. The BlackBerry Desktop Software uses the first 256 bits with AES encryption and the first 128 bits with Triple DES encryption to generate the master encryption key. The BlackBerry Desktop Software discards any unused bits.

BlackBerry Enterprise Server software versions earlier than 4.0 use a different desktop-based master encryption key generation process. See "Appendix C: Previous version of wired master encryption key generation" on page 50 for more information.

Wireless master encryption key generation process

To establish and manage master encryption keys wirelessly, the BlackBerry Enterprise Server uses the initial key establishment protocol and the key rollover protocol. Both protocols provide strong authentication: only a BlackBerry device with a valid corporate email address and an activation password can initiate wireless enterprise activation and master encryption key generation.

Protocol	Description
initial key establishment protocol	• The BlackBerry Enterprise Server uses this protocol during wireless enterprise activation to establish the initial master encryption key. • This protocol uses SPEKE to bootstrap from an activation password, enabling a BlackBerry device to establish long term public keys and a strong, cryptographically protected connection with a BlackBerry Enterprise Server.
key rollover protocol	• The BlackBerry device and the BlackBerry Enterprise Server use this protocol to regenerate a master encryption key, based on the existing master encryption key. When a user physically connects the BlackBerry device to the desktop computer, if a pending key exists, the current master encryption key on the BlackBerry device becomes a previous key and the pending key replaces the current key. If no pending key exists, the BlackBerry Desktop Software creates a new master encryption key for the user. • This protocol generates the master encryption key using existing long-term public keys and the ECMQV algorithm to negotiate a common key in such a way that an unauthorized party cannot calculate the same key. • This protocol achieves perfect forward secrecy. The new master encryption key is independent of the previous key. Knowledge of the previous master encryption key does not permit an attacker to learn the new master encryption key.

Message key

The BlackBerry Enterprise Server generates one or more message keys, which are designed to protect the integrity of data such as short keys or large messages, for each message that the BlackBerry device sends. If a message contains several datagrams and exceeds 2 KB, the BlackBerry Enterprise Server generates a unique message key for each datagram.

Each message key is comprised of random information, which makes it difficult for a third-party to decrypt, re-create, or duplicate the key.

The message key is a session key; the BlackBerry device does not store the message key persistently but frees the memory associated with it after using it in the decryption process.

Message key generation process

The BlackBerry Enterprise Server is designed to seed a DSA PRNG function to generate a message key using the following process:

1. The BlackBerry Enterprise Server obtains random data from the BlackBerry device for the seed, using a technique derived from the initialization function of the ARC4 encryption algorithm.
2. The BlackBerry Enterprise Server uses the random data to permute the contents of a 256-byte (2048-bit) state array.

   If the MSCAPI is installed on the computer on which the BlackBerry Enterprise Server software is running, the BlackBerry Enterprise Server also requests 512 bits of randomness from the MSCAPI to increase the amount of entropy.
3. The BlackBerry Enterprise Server inputs the state array into the ARC4 algorithm to further randomize the array.
4. The BlackBerry Enterprise Server draws 521 bytes from the ARC4 state array.

   Note: The BlackBerry Enterprise Server draws the additional 9 bytes (512 + 9=521) to make sure that the pointers before and after the call are not in the same place, and to take into account that the first few bytes of the ARC4 state array might not be truly random.

5. The BlackBerry Enterprise Server uses SHA512 to hash the 521-byte value to 64 bytes.
6. The BlackBerry Enterprise Server uses the 64-byte value to seed a NIST-approved DSA PRNG function. See *Federal Information Processing Standard – FIPS PUB 186-2* for more information on the DSA PRNG function.

   The BlackBerry Enterprise Server stores a copy of the seed in a file. When the BlackBerry Enterprise Server restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.
7. The DSA PRNG function generates 128 pseudo-random bits for use with Triple DES and 256 pseudo-random bits for use with AES.
8. The BlackBerry Enterprise Server uses the pseudo-random bits with the appropriate algorithm to generate the message key.

Content protection key

When you turn on or the user turns on content protection on the BlackBerry device, the BlackBerry device generates encryption keys, including the content protection key, that are designed to encrypt the user data on the BlackBerry device in the following scenarios:

Scenario	Encryption process
BlackBerry device is locked	The BlackBerry device frees the memory that it associates with the content protection key and the ECC private key that it stores in RAM. The BlackBerry device then uses the ECC public key, an asymmetric key, to encrypt new user data that it receives.
BlackBerry device is unlocked	The BlackBerry device decrypts the content protection key and the ECC private key in flash memory. The BlackBerry device then uses the ECC private key and the content protection key to decrypt user data on the BlackBerry device.

See "Protected storage of user data on a locked BlackBerry device" on page 22 for more information.

Content protection key generation process

When you turn on or the user turns on content protection of data for the first time, the following process occurs:

1. The BlackBerry device uses the NIST-approved DSA PRNG to randomly generate the content protection key, a semi-permanent 256 bit AES encryption key.
2. The BlackBerry device generates an ECC key pair.
3. The BlackBerry device prompts the user to type their BlackBerry device password.
4. The BlackBerry device derives an ephemeral 256 bit AES encryption key from the BlackBerry device password, in accordance with PKCS #5 (the password-based cryptography standard). See "Appendix E: Ephemeral AES encryption key derivation process" on page 53 for more information.
5. The BlackBerry device uses the ephemeral key to encrypt the content protection key and the ECC private key.
6. The BlackBerry device stores the encrypted content protection key, the encrypted ECC private key, and the ECC public key in flash memory.

   Note: If the user changes their BlackBerry device password, the BlackBerry device uses the new password to derive a new ephemeral key and uses the new ephemeral key to re-encrypt the encrypted versions of the content protection key and the ECC private key in flash memory.

User data encryption process on a locked BlackBerry device

1. The BlackBerry device locks. When the BlackBerry device locks for the first time after you turn on or the user turns on content protection, it uses the content protection key to automatically encrypt the bulk of its stored user and application data.
2. The BlackBerry device frees the memory associated with the decrypted content protection key and the decrypted ECC private key stored in RAM.
3. The locked BlackBerry device uses the ECC public key to encrypt data that it receives.

User data decryption process on an unlocked BlackBerry device

1. A user types the correct BlackBerry device password to unlock the BlackBerry device.
2. The BlackBerry device uses the BlackBerry device password to derive the ephemeral 256 bit AES encryption key again.
3. The BlackBerry device uses the ephemeral key to decrypt the encrypted content protection key and the encrypted ECC private key in flash memory.
4. The BlackBerry device stores the decrypted content protection key and the decrypted ECC private key in RAM.
5. If a user attempts to access user data (for example, opens a message) that the BlackBerry device encrypted while it was locked, the BlackBerry device uses the decrypted ECC private key to decrypt the user data and access the ECC-encrypted items (for example, message bodies, subjects, or recipients).
6. When the BlackBerry device has opened 128 ECC-encrypted items (typically, less than 40 messages), the BlackBerry device uses the ECC private key to decrypt the ECC-encrypted items and then re-encrypts them with the content protection key the next time that the BlackBerry device locks. If the re-encryption process is incomplete when a user next unlocks the BlackBerry device, the BlackBerry device resumes re-encryption when it locks again.
7. The BlackBerry device uses the content protection key to decrypt the user data that the content protection key encrypted.

Grand master key

When you turn on content protection of master encryption keys, the BlackBerry device uses a grand master key to encrypt the master encryption keys stored on the BlackBerry device in flash memory. When the BlackBerry device receives data encrypted with a master encryption key while it is locked, it uses the grand master key to decrypt the required master encryption key in flash memory and receive the data.

See "Protected storage of master encryption keys on a locked BlackBerry device" on page 23 for more information.

Grand master key generation process

When you turn on content protection of master encryption keys on the BlackBerry device for the first time, the following process occurs:

1. The BlackBerry device generates the grand master key, a 256 bit AES encryption key.
2. The BlackBerry device stores the decrypted grand master key in RAM.
3. The BlackBerry device uses the existing content protection key to encrypt the grand master key.
4. The BlackBerry device stores the encrypted grand master key in flash memory.
5. The BlackBerry device uses the encrypted grand master key to encrypt the master encryption keys stored in BlackBerry device flash memory.

BlackBerry symmetric key encryption algorithms

A symmetric key encryption algorithm is designed so that only the parties who know the secret key can decrypt the encrypted data or cipher text of the scrambled message.

The BlackBerry Enterprise Solution uses a symmetric key encryption algorithm to protect all data that the BlackBerry device sends or receives, while the data is in transit between the BlackBerry device and BlackBerry Enterprise Server. This standard BlackBerry encryption, which is designed to provide strong security, verifies that a BlackBerry message remains protected in transit to the BlackBerry Enterprise Server while the message data is outside the corporate firewall.

The BlackBerry Enterprise Solution uses either the Triple DES or the AES algorithm for standard BlackBerry encryption.

Encryption algorithm	Description
Triple DES	The BlackBerry Enterprise Solution uses three iterations of the DES algorithm with two 56-bit keys in outer CBC mode for an overall key length of 112 bits. See *Federal Information Processing Standard - FIPS PUB 81 [3]* for more information. In the two-key Triple DES algorithm, the first key encrypts the data, the second key decrypts the data, and then the first key encrypts the data again. Message keys and master encryption keys that the BlackBerry Enterprise Solution produces using Triple DES contain 112 bits of key data and 16 bits of parity data, which are stored as a 128-bit long binary string. Each parity bit is stored in the least significant bit of each of the 8 bytes of key data.
AES	A competition to design an algorithm with a better combination of security and performance than DES or Triple DES produced AES. AES offers a larger key size than DES or Triple DES to provide greater security against brute-force attacks. The BlackBerry Enterprise Solution uses AES with 256-bit keys in CBC mode to encrypt data that the BlackBerry Enterprise Server and the BlackBerry device send between them. The AES message keys and master encryption keys that the BlackBerry Enterprise Solution uses contain 256 bits of key data.

Software requirements for BlackBerry encryption algorithms

Encryption algorithm	BlackBerry Enterprise Server	BlackBerry Device Software	BlackBerry Desktop Software
Triple DES	any version	any version	any version
AES	4.0 or later	4.0 or later	4.0 or later

If you permit the use of both Triple DES and AES on the BlackBerry Enterprise Server and a user is running BlackBerry device software or BlackBerry Desktop Software version 3.6 and earlier, the BlackBerry Enterprise Solution generates that user's BlackBerry device master encryption keys using Triple DES.

Standard BlackBerry message encryption

Standard BlackBerry encryption is designed to encrypt messages that the BlackBerry device sends or that the BlackBerry Enterprise Server forwards to the BlackBerry device. Standard BlackBerry encryption encrypts the message

- from the time a user sends an email message from the BlackBerry device until the BlackBerry Enterprise Server receives the message
- from the time the BlackBerry Enterprise Server receives a message sent to a user until that user reads the message on the BlackBerry device

When a user sends a message from the BlackBerry device, the BlackBerry Enterprise Server does not encrypt the message when it forwards the message to the message recipient unless the user installs additional secure messaging technology on the BlackBerry device and you have enabled the BlackBerry device to use that secure messaging technology to extend the messaging security. See "Extending BlackBerry device messaging security" on page 16 for more information.

Standard BlackBerry message encryption process

When a user sends a message from the BlackBerry device, the BlackBerry device and BlackBerry Enterprise Server use symmetric key cryptography to encrypt and decrypt the message, using the following process:

1. The BlackBerry device compresses the message.
2. The BlackBerry device encrypts the message using the message key.
3. The BlackBerry device encrypts the message key using the master encryption key, which is unique to that BlackBerry device.
4. The BlackBerry device sends the encrypted message key and the encrypted message.
5. The BlackBerry Enterprise Server receives the encrypted message key and the encrypted message from the BlackBerry device.
6. The BlackBerry Enterprise Server decrypts the message key using the BlackBerry device master encryption key.
7. The BlackBerry Enterprise Server decrypts the message using the message key.
8. The BlackBerry Enterprise Server decompresses the message, and then forwards the message to the intended recipient.

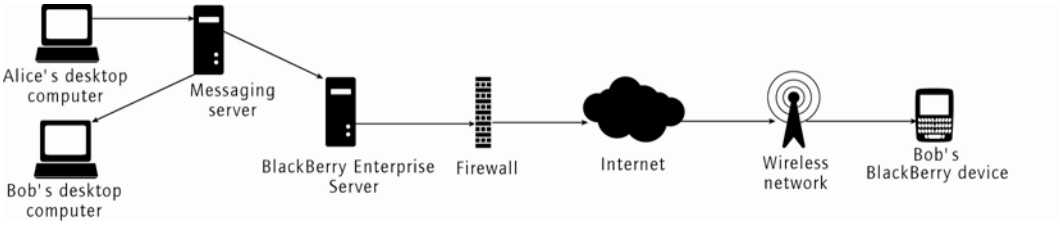
When a user receives a message, the following occurs:

1. The BlackBerry Enterprise Server receives the message.
2. The BlackBerry Enterprise Server compresses the message.
3. The BlackBerry Enterprise Server encrypts the message using the message key.
4. The BlackBerry Enterprise Server encrypts the message key using the user's BlackBerry device master encryption key.
5. The BlackBerry Enterprise Server sends the encrypted message and the encrypted message key to the user's BlackBerry device.
6. The BlackBerry device receives the encrypted message and the encrypted message key.
7. The BlackBerry device decrypts the message key using the master encryption key, which is unique to that BlackBerry device.
8. The BlackBerry device decrypts the message using the message key.
9. The BlackBerry device decompresses the message, rendering it readable by the user.

BlackBerry wireless messaging security

The BlackBerry Enterprise Solution is designed with advanced security features to work seamlessly with existing corporate networks while enabling a user to securely send and receive messages while away from their desktop computer. Email messages remain encrypted at all points between the BlackBerry device and the BlackBerry Enterprise Server.

Receiving an email message on the BlackBerry device

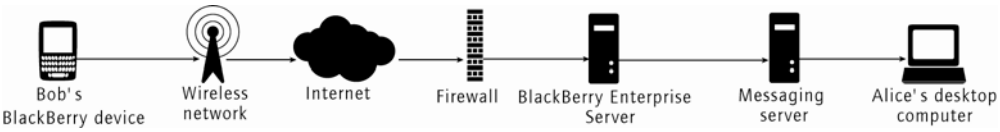


Sending a message from a desktop computer to the BlackBerry device

1. Alice sends a message to Bob from her desktop computer. Alice and Bob work at the same company.
2. The messaging server receives the email message and notifies the BlackBerry Enterprise Server that the message has arrived.
3. The messaging server delivers the message to Bob's desktop computer.
4. The BlackBerry Enterprise Server retrieves the message from the messaging server.
5. The BlackBerry Enterprise Server queries the messaging server for user preferences to determine whether or not to forward the message to Bob's BlackBerry device.
6. The BlackBerry Enterprise Server compresses and encrypts the message.
7. The BlackBerry Enterprise Server places the message in the outgoing queue.

   The BlackBerry Enterprise Server is designed to maintain a constant, direct TCP/IP connection to the wireless network over the Internet through the firewall on port 3101 (or 4101 in the case of a BlackBerry device that supports implementation alongside a WLAN). This constant connection enables the efficient, continuous delivery of data to and from the BlackBerry device.
8. The wireless network routes and then delivers the encrypted message to Bob's BlackBerry device.
9. Bob's BlackBerry device receives the encrypted message. The BlackBerry device then decrypts and displays the message for Bob to read.

Sending an email message from the BlackBerry device



Sending a message from a BlackBerry device to the desktop computer

1. Bob responds to Alice's message by composing an email on the BlackBerry device. When Bob sends the message, the BlackBerry device compresses, encrypts, and then sends the message over the wireless network.

   All messages that users create on their BlackBerry devices contain the necessary BlackBerry Enterprise Server routing information for the wireless network to make sure that the wireless network delivers the message to the appropriate BlackBerry Enterprise Server.

2. The BlackBerry Infrastructure routes the encrypted message to the BlackBerry Enterprise Server on which the user resides.

   The connection from the BlackBerry Enterprise Server to the BlackBerry Infrastructure is a two-way TCP connection on port 3101. The BlackBerry Infrastructure directs messages from the BlackBerry device to this connection using the routing information in the message.

3. The BlackBerry Enterprise Server receives the message.
4. The BlackBerry Enterprise Server decrypts, decompresses, and sends the message to the messaging server.

   The BlackBerry Enterprise Server does not store a copy of the message.

5. The messaging server delivers the message to Alice's desktop computer.

Message attachment viewing security

The BlackBerry device supports attachment viewing through the BlackBerry Attachment Service (attachment service). The attachment service enables a user to perform the following actions on their BlackBerry device:

- view Microsoft PowerPoint® slide shows, including those in .pps file format
- view .bmp, .jpg, .jpeg, .gif, .png, .tif, .tiff, and .wmf file formats
- view .doc, .dot, .txt .html, .htm, .pdf, .xls, .wpd, and .ppt documents in a browser
- open .zip files and then open any content files of supported formats
- enlarge images in .tiff format (such as scanned documents or faxes)
- access inline thumbnail images for attachments that are embedded in messages

The attachment service is designed to prevent malicious applications from accessing data on the BlackBerry device by using binary format parsing to open the attachments and prepare them to be sent to the BlackBerry device for rendering. The attachment service neither opens the attachments nor uses any third-party application to render the attachments.

PIN messaging

A PIN uniquely identifies each BlackBerry device on the wireless network. If a user knows the PIN of another BlackBerry device, they can send a PIN message to that BlackBerry device. Unlike an email message that the user sends to an email address, a PIN message bypasses the BlackBerry Enterprise Server and the corporate network.

PIN message scrambling

During the manufacturing process, Research In Motion® (RIM®) loads a common peer-to-peer encryption key onto BlackBerry devices. Although the BlackBerry device uses the peer-to-peer encryption key with Triple DES to encrypt PIN messages, every BlackBerry device can decrypt every PIN message that it receives because every BlackBerry device stores the same peer-to-peer encryption key. PIN message encryption does not prevent a BlackBerry device other than the intended recipient from decrypting the PIN message. Therefore, consider PIN messages as scrambled—but not encrypted—messages.

You can limit the number of BlackBerry devices that can decrypt your organization's PIN messages by generating a new peer-to-peer encryption key known only to BlackBerry devices in your corporation. A BlackBerry device with a corporate peer-to-peer encryption key can send and receive PIN messages with other BlackBerry devices on your corporate network with the same peer-to-peer encryption key. These PIN messages use corporate scrambling instead of the original global scrambling.

You should generate a new corporate peer-to-peer encryption key if you know the current key is compromised. You can update and resend the peer-to-peer encryption key for users in the BlackBerry Manager.

SMS and MMS messaging

SMS and MMS messaging are available on some BlackBerry devices. Supported BlackBerry devices can send SMS and MMS messages over the wireless TCP/IP connection between them. The BlackBerry device does not encrypt SMS and MMS messages.

Controlling unsecured messaging

You can control unsecured messaging (PIN, SMS, and MMS communication) in your organization using the following IT policy rules:

IT policy rule	Description
Allow External Connections	This IT policy rule controls whether applications can initiate external connections (for example, to WAP, SMS, MMS or other public gateways) on the BlackBerry device.
Confirm on Send	This IT policy rule requires a user to confirm that they wish to send the message before sending an email message, PIN message, SMS message, or MMS message.
Disable Forwarding Between Services	This IT policy rule prevents a user from forwarding or replying to a message using a different BlackBerry Enterprise Server from the one that delivered the original message. This IT policy rule also prevents using an email account to forward or reply to a PIN message or reply to an email message with a PIN message.
Disable Peer-to-Peer Normal Send	This IT policy rule prevents a user from sending plain text PIN messages when using a secure messaging package, such as the S/MIME Support Package or the PGP Support Package.

Turning off unsecured messaging

You can turn off unsecured messaging to make sure that all communication originating at the BlackBerry devices in your organization travels through the enterprise messaging environment.

Scenario	Description
turn off PIN messaging	Set the Allow Peer-to-Peer Messages IT policy rule to **False**. **Note**: When you turn off PIN messaging, users cannot send PIN messages from the BlackBerry device; however, they can still receive PIN messages on their BlackBerry devices.
turn off SMS messaging	Set the Allow SMS IT policy rule to **False**.
turn off MMS messaging	Set the Disable MMS IT policy rule to **True**.

Extending BlackBerry device messaging security

In addition to standard BlackBerry encryption, you can enable S/MIME technology or PGP technology to offer an additional layer of security between the sender and recipient of an email or PIN message. Using either one of these technologies enables sender-to-recipient authentication and confidentiality, and helps maintain data integrity and privacy from the time that a user sends a message from the BlackBerry device until the message recipient decodes and reads the message.

PGP Support Package

The PGP Support Package is designed to provide support for using OpenPGP (RFC 2440) message formatting on the BlackBerry device to enable users who already send and receive PGP protected messages in OpenPGP format using their computer email applications to send and receive PGP protected messages in that format using their BlackBerry devices.

The PGP Support Package includes tools for obtaining PGP keys and transferring them to the BlackBerry device so that BlackBerry devices with the PGP Support Package installed can decrypt PGP protected messages and users can read the decrypted messages on their BlackBerry devices. Users can digitally sign, encrypt, and send PGP protected messages from their BlackBerry devices. Without the PGP Support Package, the BlackBerry device receives PGP protected messages as unreadable cipher text.

Within the PGP Universal environment, the PGP Universal Server operates as a network appliance. The PGP Universal Server specifies secure email policies that the PGP Universal Server administrator designs. The BlackBerry device with the PGP Support Package installed enforces compliance with the PGP Universal secure email policies for all email messages.

The PGP Support Package includes support for the following:

- using the PGP Universal Server to retrieve and enforce a secure email policy
- wireless fetching of PGP keys and PGP key status using either a PGP Universal Server or an external LDAP PGP key server
- encrypting and decrypting PGP protected email and PIN messages
- verifying digital signatures on received email and PIN messages, and digitally signing outgoing email and PIN messages

The BlackBerry device is designed to use the BlackBerry MDS connection service, which resides on the BlackBerry Enterprise Server, to connect to the PGP Universal Server and to the external LDAP PGP key server(s) that the user sets on the BlackBerry device. The connection service uses a standard protocol, such as HTTP or TCP/IP, to enable the BlackBerry device to retrieve PGP keys and PGP key status from the PGP Universal Server or an external LDAP PGP key server over the wireless network.

PGP security

PGP technology is designed to enable sender-to-recipient authentication and confidentiality and help maintain data integrity and privacy from the time that the BlackBerry device user sends a message over the wireless network until the message recipient decodes and reads the message.

PGP technology relies on public key cryptography (using private and public key pairs) to provide confidentiality, integrity and authenticity.

PGP key types

The PGP Support Package uses public key cryptography with the following keys:

Key type	Description
PGP public key	The BlackBerry device uses the recipient's PGP public key to encrypt outgoing email messages, and uses the sender's PGP public key to verify digital signatures on received email messages. The PGP public key is designed to be distributed and accessed by message recipients and senders without compromising security conditions.
PGP private key	The BlackBerry device uses the PGP private key to digitally sign outgoing email messages and decrypt received email messages. Private key information should remain private to the key owner.

PGP encryption

If the PGP Support Package is installed on a BlackBerry device, when a user sends a message from that BlackBerry device, the BlackBerry device encrypts the message using the following process:

1. The BlackBerry device encrypts the message using the message recipient's PGP public key.
2. The BlackBerry device uses standard BlackBerry encryption to encrypt the PGP encrypted message.

3. The BlackBerry device sends the encrypted message to the BlackBerry Enterprise Server.
4. The BlackBerry Enterprise Server removes the standard BlackBerry encryption and sends the PGP encrypted message to the recipient.

If the PGP Support Package is installed on a BlackBerry device, when the BlackBerry device receives a message, the PGP message is encrypted with standard BlackBerry encryption and then decrypted, using the following process:

1. The BlackBerry Enterprise Server receives the PGP protected message.
2. The BlackBerry Enterprise Server uses standard BlackBerry encryption to encrypt the PGP encrypted message.
3. The BlackBerry Enterprise Server sends the encrypted message to the BlackBerry device.
4. The BlackBerry device removes the standard BlackBerry encryption and stores the PGP encrypted message.
5. When the user opens the message on the BlackBerry device, the BlackBerry device decrypts the PGP encrypted message and renders the message contents.

PGP encryption algorithms

The BlackBerry device is designed to support using a strong algorithm for PGP encryption. The PGP Allowed Content Ciphers IT policy rule default setting specifies that the BlackBerry device can use any of the supported algorithms to encrypt PGP messages. You can set the PGP Allowed Content Ciphers IT policy rule to encrypt PGP messages using any of AES (256-bit), AES (192-bit), AES (128-bit), CAST (128-bit), and Triple DES (168-bit).

The message recipient's PGP key indicates which content ciphers the recipient can support, and the BlackBerry device is designed to use one of those ciphers. The BlackBerry device encrypts the message using Triple DES by default if the recipient's PGP key does not include a list of ciphers.

See the *PGP Support Package Security Technical Overview* for more information.

S/MIME Support Package

The S/MIME Support Package is designed to enable BlackBerry device users who are already sending and receiving S/MIME messages using their computer email application to send and receive S/MIME protected messages using their BlackBerry devices. The S/MIME Support Package is designed to work with S/MIME email clients including Microsoft Outlook® and Microsoft Outlook Express, and with popular PKI components, including Netscape®, Entrust Authority™ Security Manager version 5 and later, and Microsoft CAs.

The S/MIME Support Package includes tools for obtaining certificates and transferring them to the BlackBerry device. This means that BlackBerry devices with the S/MIME Support Package installed can decrypt messages that are encrypted using S/MIME encryption and users can read the decrypted messages on their BlackBerry devices, and that users can sign, encrypt, and send S/MIME messages from their BlackBerry devices. Without the S/MIME Support Package the BlackBerry Enterprise Server sends a message to the BlackBerry device in which the message body includes a statement that the S/MIME message cannot be decrypted.

The S/MIME Support Package includes support for the following features:

- certificate and private key synchronization and management using the Certificate Synchronization Manager included in the BlackBerry Desktop Software
- encrypting and decrypting messages, including PIN messages, verifying digital signatures, and digitally signing outgoing messages
- searching for and retrieving certificates and certificate status over the wireless network using PKI protocols
- smart cards on BlackBerry devices

PKI component support

The S/MIME Support Package is designed to support the following PKI components:

- LDAP: The BlackBerry device and the Certificate Synchronization Manager use LDAP to search for and download certificates.
- OCSP: The BlackBerry device and the Certificate Synchronization Manager use OCSP to check the revocation status of a certificate on demand.
- CRL: The BlackBerry device and the Certificate Synchronization Manager obtain the most recent revocation status of certificates, which is published at a frequency set on the CA server, from a CRL.

S/MIME encryption

If the S/MIME Support Package exists on a BlackBerry device, when the BlackBerry device user sends a message, the BlackBerry device encrypts the message once with S/MIME encryption and once with standard BlackBerry encryption using the following process:

1. The BlackBerry device encrypts the message with the S/MIME certificate of the message recipient.
2. The BlackBerry device uses standard BlackBerry encryption to encrypt the S/MIME encrypted message.
3. The BlackBerry device sends the encrypted data to the BlackBerry Enterprise Server.
4. The BlackBerry Enterprise Server removes the BlackBerry standard encryption and sends the S/MIME encrypted message to the recipient.

If the S/MIME Support Package exists on a BlackBerry device, when the user receives a message on the BlackBerry device, the BlackBerry device encrypts the S/MIME message with standard BlackBerry encryption and then decrypts the message using the following process:

1. The BlackBerry Enterprise Server receives the S/MIME protected message.
2. If the message is signed-only or weakly encrypted, the BlackBerry Enterprise Server encrypts the message a second time with S/MIME encryption if you have turned on this option using the BlackBerry Manager.
3. The BlackBerry Enterprise Server uses standard BlackBerry encryption to encrypt the S/MIME data.
4. The BlackBerry Enterprise Server sends the encrypted message to the BlackBerry device.
5. The BlackBerry device removes the BlackBerry standard encryption and stores the S/MIME encrypted message.
6. When the user opens the message on the BlackBerry device, the BlackBerry device decrypts the S/MIME encrypted message and renders the message contents.

S/MIME encryption algorithms

The BlackBerry device is designed to support using a strong algorithm for S/MIME encryption. When you turn on S/MIME encryption on the BlackBerry Enterprise Server, the S/MIME Allowed Content Ciphers IT policy rule default setting specifies that the BlackBerry device can use any of the supported algorithms (other than the two weakest RC2 algorithms, RC2 (64-bit) and RC2 (40-bit)) to encrypt S/MIME messages.

You can set the S/MIME Allowed Content Ciphers IT policy rule to encrypt S/MIME messages using any of AES (256-bit), AES (192-bit), AES (128-bit), CAST (128-bit), RC2 (128-bit), Triple DES, RC2 (64-bit), and RC2 (40-bit).

If the BlackBerry device has previously received a message from the intended recipient, the BlackBerry device is designed to recall which content ciphers the recipient can support, and use one of those ciphers. The BlackBerry device encrypts the message using Triple DES by default if it does not know the decryption capabilities of the recipient.

S/MIME certificates

When a user sends an encrypted message from the BlackBerry device, the BlackBerry device uses the S/MIME certificate of the message recipient to encrypt the message.

When a BlackBerry device user receives a signed message, the BlackBerry device uses the S/MIME certificate of the message sender to verify the message signature.

S/MIME private keys

When a user sends a signed message from the BlackBerry device, the BlackBerry device uses the S/MIME private key of the user to digitally sign the message.

When a user receives an encrypted message, the BlackBerry device uses the private key of the user to decrypt the message.

See the *S/MIME Support Package White Paper* for more information.

Decrypting and reading messages on the BlackBerry device using Lotus Notes API 7.0

The BlackBerry Enterprise Server version 4.1 or later for IBM Lotus Domino with Lotus Notes API 7.0 automatically turns on support for reading IBM Lotus Notes encrypted messages and S/MIME encrypted messages on the BlackBerry device.

If a user with this feature configured on the BlackBerry device forwards or replies to an encrypted message that the BlackBerry device has received, decrypted, and decompressed, the BlackBerry Enterprise Server for IBM Lotus Domino decrypts the message before the BlackBerry device sends the message to the recipient as plain text.

Lotus Notes API 7.0 requires the user's Notes .id file and password to decrypt the received secure message. The user must manually click Import Notes ID and attach a copy of the Notes .id file that they used to login.

IBM Lotus Notes and S/MIME message decryption process

If a user configures support for reading IBM Lotus Notes and S/MIME encrypted messages on their BlackBerry device, when the user receives an IBM Lotus Notes and S/MIME encrypted message, the BlackBerry Enterprise Server for IBM Lotus Domino decrypts the message using the following process:

1. A user receives an IBM Lotus Notes and S/MIME encrypted message.
2. The BlackBerry Enterprise Server for IBM Lotus Domino messaging agent uses the user's cached Notes .id password to decrypt the message.

   If the BlackBerry Enterprise Server for IBM Lotus Domino messaging agent does not have the Notes .id password, the user must select More, More All, or Open Attachment to pull the decrypted message to the BlackBerry device.
3. The BlackBerry Enterprise Server pushes the decrypted message to the BlackBerry device, where the user can read the message.

Notes .id password protection

After a user imports the Notes .id file and password (stored in the Notes .id file), the password is

- encrypted in BlackBerry device memory using AES
- encrypted in the BlackBerry Enterprise Server for IBM Lotus Domino messaging agent memory using AES
- decrypted before being used to call the required Lotus Notes API security functions

The BlackBerry Enterprise Server for IBM Lotus Domino messaging agent deletes the Notes .id files and plain text passwords it stores when

- a message decryption failure occurs on the BlackBerry Enterprise Server

- the BlackBerry Enterprise Server restarts
- the password times out (the default expiration timeout is 24 hours)

The encrypted Notes .id password remains stored in the BlackBerry Enterprise Server for IBM Lotus Domino messaging agent memory cache.

The BlackBerry device deletes the Notes .id files and plain text passwords from BlackBerry device memory when

- a message decryption failure occurs on the BlackBerry device
- the BlackBerry device resets
- the password times out (the default expiration timeout period is 24 hours)

If a user types more than ten consecutive incorrect passwords within one hour, the BlackBerry Enterprise Server for IBM Lotus Domino messaging agent makes secure messaging unavailable to that user for one hour.

The temporary disabling period increases by ten minute increments to a limit of 24 hours. It increments each time a user exceeds the maximum number of failed password attempts and then defaults back to one hour.

When secure messaging is temporarily unavailable, a user can manually re-enable secure messaging by importing the Notes .id file, or changing their Notes .id password using the BlackBerry Desktop Software or the Domino Web Access client.

Protecting stored data

Protecting stored messages on the messaging server

The IBM Lotus Domino server and the Microsoft Exchange server perform all message storage and specific user data storage in their environments. In the Novell GroupWise server environment, the Post-Office Agent where a user's messaging account resides stores messages and user data.

Messaging server	Message storage location
IBM Lotus Domino server	IBM Lotus Domino databases within the IBM Lotus Domino environment
Microsoft Exchange server	Hidden folders in Microsoft Exchange mailboxes that are associated with a user

Storing message and user data in IBM Lotus Domino databases

The BlackBerry Enterprise Server creates and uses the following IBM Lotus Domino databases to manage BlackBerry device messages:

Database	Message storage method
BlackBerry state	• stores an entry that establishes a connection between each original message in a user's IBM Lotus Notes Inbox and the same message on that user's BlackBerry device **Note**: Each BlackBerry user has a uniquely named BlackBerry state database.
BlackBerry profiles	• stores important configuration information for each user, including the BlackBerry device identification information and master encryption key • stores a link to a user's BlackBerry state database and stores other information that the BlackBerry Enterprise Server uses to manage the flow of messages to and from the BlackBerry device

IT policy signing and storage on the BlackBerry device

An IT policy is a collection of one or more IT policy rules. An IT Admin command is a function that you can send wirelessly to immediately control access to or change ownership information on the BlackBerry device.

After the BlackBerry Enterprise Server installation process creates the BlackBerry configuration database, the BlackBerry Enterprise Server generates a unique private and public key pair to authenticate the IT policy and the IT Admin commands, and digitally signs the Default IT policy before automatically sending it and the IT policy public key to the BlackBerry device.

The BlackBerry device stores the digitally signed IT policy and the IT policy public key in the NV store in flash memory, binding the IT policy to that particular BlackBerry device. The NV store persists in flash memory and can only be overwritten by the BlackBerry device operating system. Third-party application code cannot write to the NV store.

The BlackBerry Enterprise Server stores the IT policy private key in the BlackBerry configuration database. The BlackBerry Enterprise Server uses the IT policy private key to sign all IT policy packets that it sends to the BlackBerry device. The BlackBerry device uses the IT policy public key in the NV store to authenticate the digital signature on the IT policy.

Application password encryption and storage on the BlackBerry device

A user can use the Password Keeper tool to create and store all of the passwords that they might use to gain access to applications and web sites on the BlackBerry device. This means that a user is required to remember only the Password Keeper master password to retrieve all of their stored passwords.

The first time that a user opens the Password Keeper on the BlackBerry device, they must create the Password Keeper master password. The Password Keeper encrypts the information (for example, application and web site passwords and data) that it stores using 256-bit AES, and uses the master password to decrypt the information when a user types the master password to gain access to the Password Keeper tool. The BlackBerry device automatically deletes all of its data if a user types the Password Keeper master password incorrectly ten times.

In the Password Keeper, a user can

- type a password and its identifying information (for example, which application the user can access using the password) and save the information
- generate random passwords designed to improve password strength
- copy passwords to the clipboard to be pasted into an application or web site password prompt

Protected storage of user data on a locked BlackBerry device

Content protection of user data is designed to

- use 256-bit AES to encrypt stored data when the BlackBerry device is locked
- use an ECC public key to encrypt data that the BlackBerry device receives when it is locked

When you or a user turns on content protection on the BlackBerry device, the BlackBerry device uses content protection to encrypt the following user data items:

BlackBerry device application	User data
email	• subject • email addresses • message body • attachments

BlackBerry device application	User data
calendar	• subject • location • organizer • attendees • notes included in the appointment or meeting request
MemoPad	• title • information included in the body of the note
tasks	• subject • information included in the body of the task
contacts	• all information except the title and category
AutoText	• all text that automatically replaces the text a user types
BlackBerry Browser	• content that web sites or third-party applications push to the BlackBerry device • web sites that the user saves on the BlackBerry device • browser cache

Enabling protected storage of BlackBerry device data

You enable protected storage of data on the BlackBerry device by setting the Content Protection Strength IT policy rule. Choose a strength level that corresponds to the desired ECC key strength.

If a user turns on content protection on the BlackBerry device, in the BlackBerry device Security options), the BlackBerry device sets the content protection strength to level 0 (to use a 160-bit ECC key strength) by default.

When the content-protected BlackBerry device decrypts a message that it received while locked, the BlackBerry device uses the ECC private key in the decryption operation. The longer the ECC key, the more time the ECC decryption operation adds to the BlackBerry device decryption process. Choose a content protection strength level that optimizes either the ECC encryption strength or the decryption time.

If you set the content protection strength to level 1 (to use a 283-bit ECC key) or to level 2 (to use a 571-bit ECC key), RIM recommends that you set the Minimum Password Length IT policy rule to enforce a minimum BlackBerry device password length of 12 characters or 21 characters, respectively. These password lengths maximize the encryption strength that the longer ECC keys are designed to provide. The BlackBerry device uses the BlackBerry device password to generate the ephemeral 256-bit AES encryption key that the BlackBerry device uses to encrypt the content protection key and the ECC private key. A weak password produces a weak ephemeral key.

See "Content protection key generation process" on page 10 for more information.

Protected storage of master encryption keys on a locked BlackBerry device

If you turn on content protection of master encryption keys, the BlackBerry device uses the grand master key to encrypt the master encryption keys stored in flash memory and stores the decrypted grand master key in RAM. When you, the user, or a configured password timeout locks the BlackBerry device, the wireless radio remains on and the BlackBerry device does not free the memory associated with the grand master key. When the BlackBerry device receives data encrypted with a master encryption key while it is locked, it uses the decrypted grand master key to decrypt the required master encryption key in flash memory and receive the data.

See "Grand master key generation process" on page 11 for more information.

Enabling protected storage of master encryption keys on a locked BlackBerry device

You enable protected storage of master encryption keys on the BlackBerry device by setting the Force Content Protection of Master Keys IT policy rule. When you turn on content protection of master encryption keys, the BlackBerry device uses the same ECC key strength that it uses to encrypt user and application data when encrypting the master encryption keys.

See "Enabling protected storage of BlackBerry device data" on page 23 for more information.

Protected storage of master encryption keys on a BlackBerry device during a reset

If you turn on content protection of master encryption keys, during a BlackBerry device reset the BlackBerry device

- turns off the wireless radio
- turns off serial bypass
- frees the memory associated with all data and encryption keys stored in RAM, including the decrypted grand master key
- locks

The wireless radio and serial bypass are designed to be turned off while the content protection key is not available to decrypt the grand master key in flash memory. Until a user unlocks the BlackBerry device using the correct BlackBerry device password the BlackBerry device cannot receive and decrypt data.

When the user unlocks the BlackBerry device after a reset, the BlackBerry device

- uses the content protection key to decrypt the grand master key in flash memory
- stores the decrypted grand master key in RAM again
- re-establishes the wireless connection to the BlackBerry Infrastructure
- resumes serial bypass
- receives data from the BlackBerry Enterprise Server

Cleaning the BlackBerry device memory

By default, the BlackBerry device continually runs a standard Java garbage collection process to reclaim BlackBerry device memory that is no longer referenced.

If secure garbage collection is turned on, the BlackBerry device performs the following additional actions:

- overwrites the memory reclaimed by the standard garbage collection process with zeroes
- periodically runs the memory cleaner program, which tells BlackBerry device applications to empty any caches and free memory associated with unused, sensitive application data
- automatically overwrites the memory freed by the memory cleaner program when it runs

Any of the following conditions enable the BlackBerry device to perform secure garbage collection:

- content protection is turned on
- a program uses the RIM Cryptographic Application Programming Interface (Crypto API) to create a private or symmetric key
- a third-party application turns on secure garbage collection by registering with the memory cleaner
- S/MIME Support Package is installed
- PGP Support Package is installed

Configuring memory cleaning

Users can configure the memory cleaner program to run when their BlackBerry devices are holstered or when their BlackBerry devices remain idle for a configured period of time. Users can also manually run the memory cleaner program on their BlackBerry devices or run specific registered memory cleaners in the BlackBerry device Security options. If secure garbage collection is turned on, when the memory cleaner program runs, it invokes the secure garbage collection process.

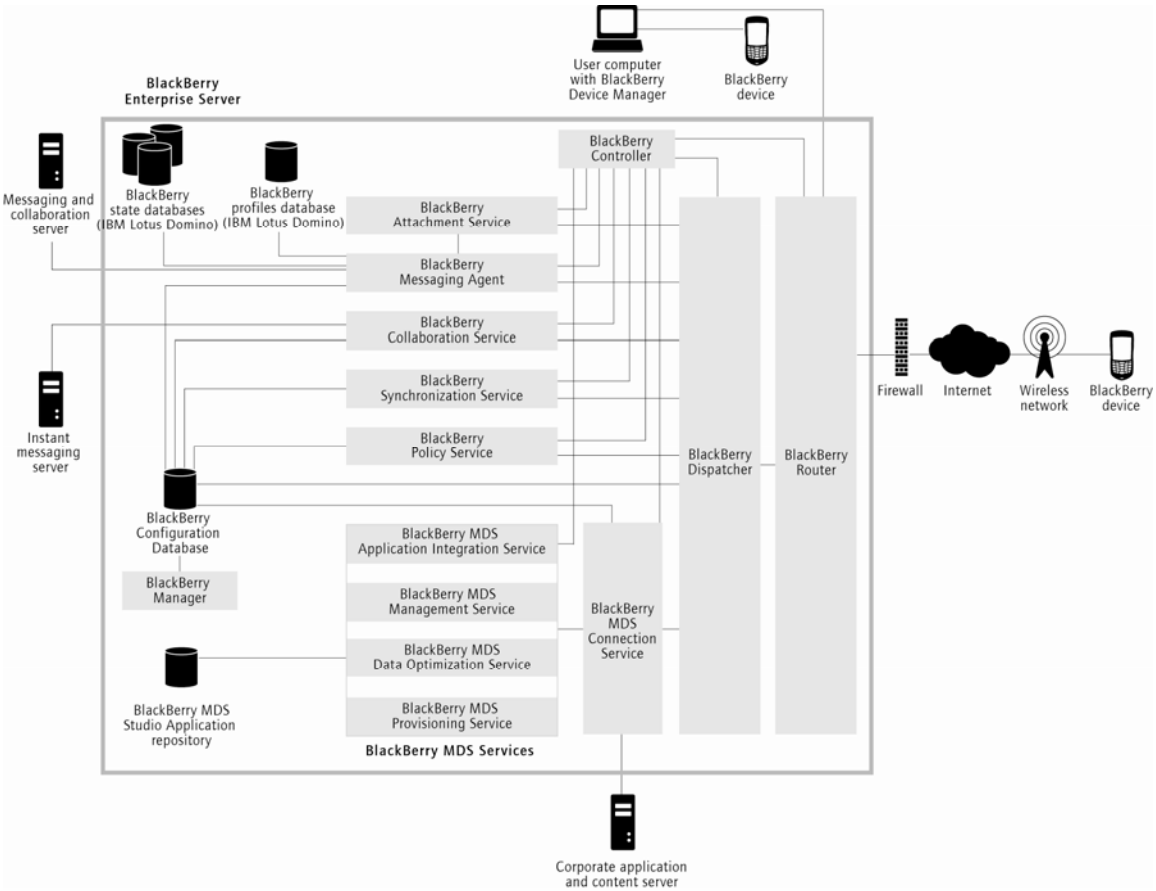
You can configure the memory cleaner program to run automatically when the

- user synchronizes the BlackBerry device with the desktop computer
- user locks the BlackBerry device
- BlackBerry device locks after a specified amount of idle time
- user changes the time or time zone on the BlackBerry device

See the *Policy Reference Guide* for more information.

BlackBerry architecture component security

The BlackBerry Enterprise Server consists of services that provide functionality and components that monitor services and processes, route, compress, and encrypt data, and communicate with the BlackBerry Infrastructure over the wireless network.



BlackBerry Enterprise Server architecture

See the *BlackBerry Enterprise Server Feature and Technical Overview* for more information on the BlackBerry Enterprise Server architecture.

BlackBerry Infrastructure

The BlackBerry Infrastructure is designed to communicate with the BlackBerry Enterprise Server using a RIM-proprietary protocol called Server Routing Protocol (SRP). SRP is a point-to-point protocol that runs over TCP/IP.

BlackBerry Enterprise Server

The BlackBerry Enterprise Server is designed to establish a secure, two-way link between a user's corporate email account and that user's BlackBerry device. The BlackBerry Enterprise Server uses this link to complete message delivery within the protection of the corporate firewall.

Messaging server

The BlackBerry Enterprise Solution is designed to interoperate with messaging servers such as Microsoft Exchange, IBM Lotus Domino, and Novell GroupWise. The BlackBerry Enterprise Solution is designed to use existing messaging server security without altering the normal functionality of the messaging server. The messaging server continues to receive, deliver, and store all corporate email messages, while the BlackBerry Enterprise Server acts as a conduit to transfer these messages to and from the BlackBerry device.

BlackBerry configuration database

The BlackBerry services that do not connect to the messaging server directly access the configuration information that a SQL database (the BlackBerry configuration database) stores. BlackBerry services that might otherwise require access to the messaging server can access encryption keys and passwords through the BlackBerry configuration database to perform many tasks.

The BlackBerry configuration database stores the following information:

- BlackBerry Enterprise Server names
- unique SRP authentication keys and unique SRP IDs, or UIDs, that each BlackBerry Enterprise Server uses in the SRP authentication process to establish a connection to the wireless network
- IT policy private keys of the IT policy public and private key pair that the BlackBerry Enterprise Server generates for each BlackBerry device
- PIN of each BlackBerry device
- read-only copies of each unique BlackBerry device master encryption key
- user lists
- information contained in the message header that the BlackBerry Enterprise Server sends, for example, message ID, date, and message status, (BlackBerry Enterprise Server for IBM Lotus Domino only)
- a semi-permanent reference to user data using the GroupWise MessageID in the MBMailSync, MBCalendarSync, MBPIMSync, and MBFolderSync database synchronization tables (BlackBerry Enterprise Server for Novell GroupWise only)

Protecting the BlackBerry configuration database

Your environment might benefit from configuring the Microsoft SQL Server for optimal security of the BlackBerry configuration database and protection of the stored user encryption keys.

Configuration option	Recommendations
shield your Microsoft SQL Server installation from Internet-based attacks	• Require Windows Authentication Mode for connections to Microsoft SQL Server to restrict connections to Microsoft Windows® user and domain user accounts and enable credentials delegation. **Note**: Windows Authentication Mode eliminates the need to store passwords on the client side. However, if you are running BlackBerry MDS Services, your SQL server must support Mixed Mode authentication. • Use Windows security enforcement mechanisms such as stronger authentication protocols and mandatory password complexity and expiration.
password-protect the service account	• Assign a string password to your sa account, even on servers that require Windows Authentication. **Note**: A string password is designed to prevent exposure of a blank or weak sa password if the server is ever reconfigured for Mixed Mode Authentication.
limit the privilege level of Microsoft SQL Server Windows services	• Associate each service with a Windows account from which the service derives its security context. **Note**: Microsoft SQL Server allows a user of the sa login and in some cases other users to access operating system features derived from the security context of the account that owns the server process. If the server is not secured, a malicious user might use these operating system calls to extend an attack to any other resource to which the Microsoft SQL Server service account has access.
use the Microsoft SQL Server Enterprise Manager	• If you must change the account associated with a Microsoft SQL Server service, use the SQL Server Enterprise Manager. The SQL Server Enterprise Manager sets the appropriate permissions on the files and registry keys that the Microsoft SQL Server uses. • Do not use the Microsoft Management Console Services applet to change the account associated with a Microsoft SQL Server service. Using this Services applet requires you to manually adjust many registry and NTFS file system permissions and Microsoft Windows user rights. **Note**: See the Microsoft Knowledge Base article *How to change the SQL Server or SQL Server Agent service account without using SQL Enterprise Manager in SQL Server 2000 or SQL Server Management Studio in SQL Server 2005*.
make the Microsoft SQL Server ports that are monitored by default on your firewall unavailable	• Configure your firewall to filter out packets that are addressed to TCP port 1433, addressed to UDP port 1434, or associated with named instances.
use a secure file system	• Use NTFS for the Microsoft SQL Server because it is more stable and recoverable than FAT file systems, and enables security options such as file and directory ACLs and EFS. • Do not change the permissions that the Microsoft SQL Server sets during installation. The Microsoft SQL Server sets appropriate ACLs on registry keys and files if it detects NTFS. • If you must change the account that runs the Microsoft SQL Server, decrypt the files under the old account and re-encrypt them under the new account.

Configuration option	Recommendations
delete unsecured, old setup files	• Delete Microsoft SQL Server setup files that might contain plain text, credentials encrypted with weak public keys, or sensitive configuration information that the Microsoft SQL Server logged to a Microsoft SQL Server version-dependent location during installation. **Note**: Microsoft distributes a free tool, Killpwd, which is designed to locate and remove passwords from unsecured, old setup files on your system. See the Microsoft Knowledge Base article *Service Pack Installation May Save Standard Security Password in File* for more information.
audit connections to the Microsoft SQL Server	• At a minimum, log failed connection attempts to the Microsoft SQL Server and review the log regularly. • When possible, save log files to a different hard drive than the one on which data files are stored.

Changing the BlackBerry configuration database

If you move the BlackBerry device to a BlackBerry Enterprise Server that uses a different BlackBerry configuration database, you or a user must erase all user and application data, the BlackBerry device master encryption key, and the IT policy public key from the BlackBerry device. See "Erasing data from BlackBerry device memory and making the BlackBerry device unavailable" on page 43 for more information.

You or the user must initiate regeneration of a new, unique master encryption key. The new BlackBerry Enterprise Server must generate a unique IT policy private and public key pair and digitally sign and send the Default IT policy and the IT policy public key to the BlackBerry device before the BlackBerry device can communicate with the new BlackBerry Enterprise Server.

The new BlackBerry configuration database stores the new BlackBerry Enterprise Server name and the BlackBerry device master encryption key and IT policy private key.

BlackBerry MDS Services databases

The BlackBerry MDS Services store their database access credentials in plain text form in INSTALL_DIR\BlackBerry MDS Services 4.1.0\jakarta-tomcat-5.5.9\conf\server.xml. To protect the access credentials in that storage location, you must

- use a separate SQL login account to install and manage the BlackBerry MDS Services databases
- assign read and write control to that location to a separate BlackBerry MDS Services SQL login account only

See the *BlackBerry Enterprise Server Installation Guide* for more information.

Protecting the BlackBerry Infrastructure connections

The BlackBerry Enterprise Server is designed to communicate with the BlackBerry Infrastructure using SRP authentication to establish a connection to the wireless network. The BlackBerry Enterprise Server contacts the BlackBerry Infrastructure to establish an initial connection using SRP.

The BlackBerry Enterprise Server and the BlackBerry Infrastructure perform an authentication handshake when they attempt to establish a connection. If the authentication fails, they do not establish a connection. If a BlackBerry Enterprise Server uses the same unique SRP authentication key and unique SRP ID to connect to (and then disconnect from) the BlackBerry Infrastructure five times in one minute, the BlackBerry Infrastructure disables that SRP ID to prevent a malicious user using the same SRP ID (for example, to try to create a Denial of Service condition).

After the BlackBerry Enterprise Server and the BlackBerry Infrastructure establish an initial connection over the Internet, the BlackBerry Enterprise Server uses a persistent TCP/IP connection to send data to the BlackBerry Infrastructure. The BlackBerry Infrastructure uses standard protocols to send data to the BlackBerry device.

A BlackBerry device can bypass SRP connectivity and authentication by using the BlackBerry Router to connect directly to the BlackBerry Enterprise Server. The BlackBerry Enterprise Server can communicate with the BlackBerry Router using a combination of the SRP and BlackBerry Router authentication protocols.

SRP authentication

SRP is designed to perform the following actions when the BlackBerry Enterprise Server and BlackBerry Infrastructure establish an authenticated connection and subsequently transfer data between them.

SRP action	Description
authenticate the BlackBerry Infrastructure to the BlackBerry Enterprise Server and the BlackBerry Enterprise Server to the BlackBerry Infrastructure	The BlackBerry Infrastructure and the BlackBerry Enterprise Server authenticate with each other before they can transfer data. The authentication handshake sequence depends on a shared secret encryption key (the SRP authentication key) on both the BlackBerry Enterprise Server and the BlackBerry Infrastructure. If at any point in the authentication handshake sequence the authentication fails, SRP terminates the connection.
exchange configuration information between the BlackBerry Enterprise Server and the BlackBerry Infrastructure	The BlackBerry Enterprise Server is designed to send a basic information packet to the BlackBerry Infrastructure immediately following the initial SRP authentication process. The packet format is designed to be recognizable to both the BlackBerry Enterprise Server and the BlackBerry Infrastructure, enabling both sides to configure the parameters of the SRP implementation dynamically. To support backward compatibility with older versions of the BlackBerry Enterprise Server software, which terminate the SRP connection if they receive unrecognized packets, the BlackBerry Infrastructure does not send basic information packets to the BlackBerry Enterprise Server until the BlackBerry Enterprise Server has sent a packet of the same format to the BlackBerry Infrastructure.
send and receive transactions between the BlackBerry Enterprise Server and the BlackBerry Infrastructure	If the connection between the BlackBerry Enterprise Server and the BlackBerry Infrastructure terminates, the wireless network can queue up to five undelivered messages for up to seven days. If there are more than five pending messages, the BlackBerry Enterprise Server stores them in the BlackBerry configuration database. The BlackBerry Infrastructure does not store data to send to BlackBerry devices. If the BlackBerry Infrastructure is not operational, the wireless network discards the pending messages—the BlackBerry device does not receive the message and the BlackBerry Enterprise Server does not receive an acknowledgement packet from the recipient BlackBerry device. When the BlackBerry Infrastructure is operational again, the BlackBerry Enterprise Server resends messages for which it did not receive an acknowledgement packet from a recipient.

SRP authentication process

Step	Action	Description
1	The BlackBerry Enterprise Server sends its SRP ID, or UID, to the BlackBerry Infrastructure.	The BlackBerry Enterprise Server sends a packet to the BlackBerry Infrastructure to claim its own UID.
2	The BlackBerry Infrastructure sends a challenge string to the BlackBerry Enterprise Server.	The BlackBerry Infrastructure sends a random challenge string to the BlackBerry Enterprise Server.

Step	Action	Description
3	The BlackBerry Enterprise Server sends a challenge string to the BlackBerry Infrastructure.	When the BlackBerry Enterprise Server receives the BlackBerry Infrastructure challenge string, it sends a challenge string to the BlackBerry Infrastructure.
4	The BlackBerry Infrastructure sends a challenge response to the BlackBerry Enterprise Server.	The BlackBerry Infrastructure hashes the BlackBerry Enterprise Server challenge string with the SRP authentication key, a 20-byte shared secret encryption key, using the keyed HMAC with SHA1. The BlackBerry Infrastructure sends the resulting 20-byte value back to the BlackBerry Enterprise Server.
5	The BlackBerry Enterprise Server sends a challenge response to the BlackBerry Infrastructure.	The BlackBerry Enterprise Server responds to the BlackBerry Infrastructure challenge string by hashing the challenge with the shared SRP authentication key.
6	The BlackBerry Infrastructure sends an acceptance to the BlackBerry Enterprise Server.	When the BlackBerry Infrastructure accepts the challenge response, it sends a final confirmation to the BlackBerry Enterprise Server to complete the authentication process and set up an authenticated SRP connection between the BlackBerry Infrastructure and the BlackBerry Enterprise Server. If the BlackBerry Infrastructure rejects the response, the connection fails and SRP ends the authentication session.

BlackBerry Router protocol authentication

The BlackBerry Router is designed to bypass the SRP authenticated connection to the BlackBerry Infrastructure to route data to BlackBerry devices that are connected to the BlackBerry Device Manager through a physical connection to a desktop computer. Data between the BlackBerry devices and the BlackBerry Router is compressed and encrypted.

You can install the BlackBerry Router on a remote computer to route data traffic between the BlackBerry Infrastructure and one or more BlackBerry Enterprise Servers. The BlackBerry device must authenticate itself to the BlackBerry Enterprise Server to prove that it knows the master encryption key before the BlackBerry Router sends data to the BlackBerry device.

When the BlackBerry Router protocol authentication is successful, the BlackBerry device sends data to the BlackBerry Router through the BlackBerry Device Manager, and the BlackBerry Router sends data to the BlackBerry device through the BlackBerry Device Manager. When the user disconnects the BlackBerry device from the desktop computer or closes the BlackBerry Device Manager, the wireless data flow over the SRP connection is restored.

BlackBerry Router protocol authentication process

Step	Action	Description
1	A user physically connects a BlackBerry device to a desktop computer.	The user connects the BlackBerry device to a desktop computer that is running the BlackBerry Device Manager.

Step	Action	Description
2	The BlackBerry Router authenticates the BlackBerry device.	The BlackBerry Router uses its unique authentication protocol to verify that the BlackBerry device has the correct master encryption key. The value of the master encryption key that the BlackBerry device and the BlackBerry Enterprise Server share is not available to the BlackBerry Router. The BlackBerry Enterprise Server and the BlackBerry device use the same authentication information to validate each other that the SRP authentication handshake sequence uses to determine whether or not the BlackBerry Enterprise Server can connect to the BlackBerry Infrastructure.

Wireless enterprise activation authentication

Wireless enterprise activation enables a user to activate a BlackBerry device on the BlackBerry Enterprise Server without a physical connection to a desktop computer. You can use wireless enterprise activation to implement a large number of BlackBerry devices remotely.

Wireless enterprise activation produces a master encryption key that authenticates a user and secures the communication between the BlackBerry Enterprise Server and the BlackBerry device. The BlackBerry Enterprise Server and the BlackBerry device use an initial key establishment protocol that makes use of SPEKE to bootstrap from an activation password to establish a shared master encryption key that enables strong authentication between them.

After the BlackBerry device successfully activates on the BlackBerry Enterprise Server, the BlackBerry device no longer requires the activation password. The user (or another user) cannot reuse that password to activate another BlackBerry device.

Note: A WLAN implementation of the BlackBerry Enterprise Solution does not support wireless enterprise activation.

Wireless enterprise activation authentication process

Step	Action	Description
1	A user initiates the wireless enterprise activation process.	The user opens the enterprise activation program on the BlackBerry device and types their corporate email address and the activation password that you communicated to them.
2	The BlackBerry device sends an activation request to the BlackBerry Infrastructure.	The BlackBerry device sends an activation request to the BlackBerry Infrastructure using standard BlackBerry protocols. The BlackBerry Infrastructure uses SMTP to send an activation message to the user's corporate email account. This activation message contains BlackBerry device routing information and public keys.
3	The BlackBerry Enterprise Server sends an activation response to the BlackBerry device.	The BlackBerry Enterprise Server sends the BlackBerry device an activation response that contains BlackBerry Enterprise Server routing information and public keys.

Step	Action	Description
4	The BlackBerry Enterprise Server and the BlackBerry device establish and verify the shared master encryption key.	The BlackBerry Enterprise Server and the BlackBerry device use the initial key establishment protocol to establish a master encryption key. The BlackBerry Enterprise Server and the BlackBerry device verify the master encryption key with each other. If the BlackBerry Enterprise Server and the BlackBerry device mutually confirm the correct master encryption key, the activation proceeds, and the BlackBerry Enterprise Server and the BlackBerry device use the master encryption key to encrypt further communication between them.
5	The BlackBerry Enterprise Server sends service books to the BlackBerry device.	The BlackBerry Enterprise Server sends the appropriate service books to the BlackBerry device. The user can now send messages from and receive messages on the BlackBerry device.
6	The BlackBerry Enterprise Server sends data to the BlackBerry device.	If wireless PIM synchronization and wireless backup is enabled for the user, the BlackBerry Enterprise Server sends the following data to the user's BlackBerry device: • calendar entries • contacts, tasks, and memos • existing BlackBerry device options (if applicable) that the BlackBerry device backed up using automatic wireless backup.

See the *BlackBerry Wireless Enterprise Activation Technical Overview* for more information.

TCP/IP connection

The TCP/IP connection from the BlackBerry Enterprise Server to the BlackBerry Router is designed to be secure in the following ways:

Security measure	Description
The BlackBerry Enterprise Server sends outbound traffic to the BlackBerry device only through the authenticated connection to the BlackBerry Infrastructure.	• You must configure your corporate firewall or proxy to permit the BlackBerry Enterprise Server to initiate and maintain an outbound connection to the BlackBerry Infrastructure on TCP port 3101.
The BlackBerry Enterprise Server does not send inbound-initiated traffic to the messaging server.	• The BlackBerry Enterprise Server discards inbound traffic from any source other than the BlackBerry device (through the BlackBerry Infrastructure or BlackBerry Desktop Software) or the messaging server.

Security measure	Description
The BlackBerry Enterprise Solution encrypts data traffic over TCP/IP.	• Data remains encrypted with standard BlackBerry encryption from the BlackBerry Enterprise Server to the BlackBerry device or from the BlackBerry device to the BlackBerry Enterprise Server. There is no intermediate point at which the data is decrypted and encrypted again. • No data traffic of any kind can occur between the BlackBerry Enterprise Server and the wireless network or the BlackBerry device unless the BlackBerry Enterprise Server can decrypt the data using the correct, valid master encryption key. Only the BlackBerry device and BlackBerry Enterprise Server have the correct, valid master encryption key.
The BlackBerry Enterprise Server encrypts data traffic between specific components	• The BlackBerry Enterprise Server encrypts data traffic between specific components. The BlackBerry Collaboration Service, the connection service, the BlackBerry Policy Service, and the BlackBerry Synchronization Service share a secure communication password that is known only to them. The BlackBerry Messaging Agent and the BlackBerry Dispatcher share a different secure communication password that is known only to them. When one of these components initiates a connection to the BlackBerry Dispatcher, the BlackBerry inter-process protocol uses SPEKE to bootstrap from the component's secure communication password and establishes a 256-bit AES encryption key (a session key). The BlackBerry Enterprise Server then uses the session key to encrypt data traffic to any components that store the same secure communication password.
The BlackBerry device initiates inbound connections using the BlackBerry Router to a WLAN only.	• The BlackBerry Router sends the Internet or intranet content requests from the BlackBerry device over port 4101 to the WLAN. The BlackBerry Router verifies that the PIN belongs to a valid BlackBerry device that is registered on the wireless network.

Messaging server to desktop email program connection

You can encrypt the BlackBerry device data in transit between the messaging server and the user's desktop email program.

Messaging server	Data traffic encryption method
IBM Lotus Domino	• The BlackBerry Enterprise Server and the IBM Lotus Domino server communicate using the same IBM Lotus Notes RPC to enable seamless communication between the BlackBerry Enterprise Server, BlackBerry-related IBM Lotus Domino databases, and the IBM Lotus Domino server. • A user that provisions their BlackBerry device using a physical connection to their desktop computer can encrypt data traffic in transit between the IBM Lotus Domino server and their IBM Lotus Notes Inbox. See the IBM Lotus Domino help files for more information.

Messaging server	Data traffic encryption method
Microsoft Exchange	• The BlackBerry Enterprise Server and the Microsoft Exchange Server communicate using the same Microsoft Exchange server RPC. • A user can use 128-bit encryption to encrypt RPC communication over the MAPI connection between the Microsoft Exchange Server and Microsoft Outlook. See the Microsoft product documentation for more information on enabling encryption in Microsoft Windows.
Novell GroupWise	• The BlackBerry Enterprise Server for Novell GroupWise is designed to use a trusted application key to open a connection to the GroupWise server. To generate the trusted application key, the GroupWise administrator runs the trusted application key generator, specifies the GroupWise primary domain database location, and then specifies the application name that the BlackBerry Enterprise Server should use to connect to the GroupWise server. The trusted application key is a 64-byte ASCII string. The BlackBerry Enterprise Server connects securely to a user's mailbox using the trusted application name and key. The GroupWise server verifies the trusted application name and key and permits the BlackBerry Enterprise Server to establish a connection to the user's GroupWise database.

BlackBerry Mobile Data System connections

A user can use the BlackBerry Browser and third-party Java applications on the BlackBerry device to access the Internet and your organization's intranet and to accept and respond to push requests from BlackBerry Enterprise Server-side push applications. The BlackBerry MDS uses standard Internet protocols such as HTTP or TCP/IP to access data on the Internet or corporate intranet. The BlackBerry device uses standard BlackBerry encryption to protect the online corporate data, applications, and data from the Internet that a user receives on their BlackBerry device.

Protecting the HTTP connection

If an application on the BlackBerry device accesses servers on the Internet, you can set up an HTTP connection that uses TLS/SSL, an HTTPS protocol, to provide additional authentication and security. The BlackBerry device supports HTTPS communication in the following modes:

HTTPS protocol	BlackBerry MDS encryption method	Description
proxy mode TLS/SSL	Sun® JSSE 1.4.1 cipher suite components	• The connection service sets up the proxy mode TLS/SSL connection on behalf of the BlackBerry device. • The BlackBerry device does not use proxy mode TLS/SSL to encrypt data traffic over the wireless network; standard BlackBerry encryption encrypts the data traffic between the BlackBerry device and BlackBerry Enterprise Server. Data traffic is therefore encrypted over the wireless network unless it is behind the corporate firewall. • The BlackBerry device experiences faster response times using this protocol than with handheld mode TLS/SSL.

HTTPS protocol	BlackBerry MDS encryption method	Description
handheld mode TLS/SSL	TLS and WTLS key establishment algorithms, symmetric ciphers and hash algorithms that the RIM Crypto API currently supports on the BlackBerry device	• The BlackBerry device uses handheld (direct) mode TLS/SSL to encrypt data for the entire connection between the BlackBerry device and the content server. • Data traffic over the wireless network remains encrypted and is not decrypted at the connection service. • Use handheld mode TLS/SSL when only the endpoints of the transaction are trusted (for example, with banking services). **Note**: BlackBerry devices with BlackBerry Device Software version 3.6.1 or later support BlackBerry device handheld mode TLS/SSL connections.

WAP gateway connections

BlackBerry Device Software version 3.2.1 or later supports WTLS, which is designed to provide an extra layer of security when connecting to a WAP gateway. WTLS requires a WAP gateway to provide standard WAP access to the Internet. To use a WAP gateway, your company must work with the network operator or service provider.

Authenticating a user

When a user receives a new BlackBerry device, the BlackBerry Enterprise Solution uses either a desktop-based or wireless master encryption key generation method to authenticate the user and their BlackBerry device to the BlackBerry Enterprise Server. The user must have a valid email address for their BlackBerry device to activate successfully and register with the wireless network.

Authenticating a user to a BlackBerry device using a password

When you add a BlackBerry device to a BlackBerry Enterprise Server, you can require a user to authenticate to the BlackBerry device using a security password. You can use IT policy rules to configure features such as password duration, length, and strength, to require password patterns, and to forbid specific passwords. See the *Policy Reference Guide* for more information.

If the user intends to activate their BlackBerry device wirelessly, they must contact you for a temporary activation password that the BlackBerry device uses to establish the master encryption key. You can set the BlackBerry device activation password and communicate it to the user.

The activation password

- applies to that user's email account only
- is not valid after five unsuccessful activation attempts
- expires if a user does not activate the BlackBerry device within the default period of 48 hours, or a period of up to 720 hours that you configure after you create their activation password
- is removed from the BlackBerry Enterprise Server when the BlackBerry device activates successfully

Authenticating a user using a smart card

Use two-factor authentication, using a smart card, to require users to prove their identity to the BlackBerry device by two factors:

- what they have (the smart card)

- what they know (their smart card password).

The BlackBerry Smart Card Reader integrates smart card use with the BlackBerry Enterprise Solution, enabling a user to authenticate with their smart card to login to certain Bluetooth-enabled BlackBerry devices.

The BlackBerry Smart Card Reader

- creates a reliable two-factor authentication environment for granting users access to BlackBerry and PKI applications
- is designed to enable the wireless digital signing and encryption of wireless email messages using the S/MIME Support Package
- stores all encryption keys in RAM only and never writes the keys to flash memory

See the *BlackBerry Smart Card Reader Security White Paper* for more information.

Binding the smart card to the BlackBerry device

If a user has a smart card authenticator, smart card driver, and smart card reader driver installed on their BlackBerry device, either you or that user can initiate two-factor authentication on the BlackBerry device to bind the BlackBerry device to the installed smart card. After the BlackBerry device binds to the smart card, it requires that smart card to authenticate the user.

You can set the Force Smart Card Two-Factor Authentication IT policy rule in the BlackBerry Manager to require that a user authenticates with the BlackBerry device using a smart card. If you do not force the user to authenticate with the BlackBerry device using a smart card, the user can turn two-factor authentication on and off with their smart card by setting the User Authenticator field in the BlackBerry device Security Options.

When you or the user enables two-factor authentication, the following events occur:

1. The BlackBerry device locks.
2. When a user tries to unlock the BlackBerry device, the BlackBerry device prompts the user to type the BlackBerry device password. If the user has not yet set a BlackBerry device password, the BlackBerry device forces them to set one.
3. The BlackBerry device prompts the user to type the user authenticator (smart card) password to turn on two-factor authentication with the installed smart card.
4. The BlackBerry device binds to the installed smart card automatically by storing the following smart card binding information in a special BlackBerry device NV store location that is inaccessible to a user:
    - name of a Java class required by the BlackBerry Smart Card Reader
    - format of the binding information (currently, a version byte with a value of 0)
    - type of smart card (for the Common Access Card, this string is "GSA CAC")
    - name of a Java class required by the smart card code
    - unique 64-bit identifier that the smart card provides
    - smart card label that the smart card provides (for example, "GRAHAM.JOHN.1234567890")
5. The BlackBerry device pushes the current IT policy to the BlackBerry Smart Card Reader.

Confirming that the BlackBerry device is bound to the correct smart card

After a user turns on two-factor authentication, whenever the BlackBerry device prompts the user to insert the smart card into the BlackBerry Smart Card Reader, the BlackBerry device prompt indicates the label and the card type of the correct (bound) smart card. If the BlackBerry device is running BlackBerry Device Software version 3.6 or earlier with either the S/MIME Support Package version 1.5 installed or no S/MIME Support Package installed, the information in the prompt is the only indication that a smart card is bound to the BlackBerry device.

If the BlackBerry device is running either BlackBerry Device Software version 3.6 or earlier with the S/MIME Support Package version 4.0 or later installed or BlackBerry Device Software version 4.0 or later (S/MIME Support Package optional), the user can also view smart card information in the BlackBerry device Security Options.

Field	Description
Name	indicates the type of the installed smart card
Initialized	indicates whether the BlackBerry device is authenticated with and bound to the smart card • a value of Yes indicates that the BlackBerry device is bound to the smart card • a value of No indicates that the BlackBerry device is not bound to the smart card

Controlling BlackBerry devices

With the BlackBerry Enterprise Solution, you can monitor and control all BlackBerry devices wirelessly from the BlackBerry Manager.

Controlling BlackBerry device behaviour using IT policy rules

Use one or more IT policies to control the behavior of BlackBerry devices and the BlackBerry Desktop Software in your organization.

The Default IT policy includes all standard IT policy rules on the BlackBerry Enterprise Server. When new users in a BlackBerry Domain complete activation of their BlackBerry devices on the BlackBerry Enterprise Server, the BlackBerry Enterprise Server automatically pushes the Default IT policy to their BlackBerry devices. The standard IT policy rules do not enforce the default BlackBerry device or BlackBerry Desktop Software behavior. You can use either of the following methods to change the default behavior of BlackBerry devices and BlackBerry Desktop Software in your organization:

- set the values of IT policy rules in the Default IT policy
- create a new IT policy, set its IT policy rule values, and assign one or more users or user groups to the new IT policy

Changing the default behavior

An IT policy rule enables you to customize and control BlackBerry device and BlackBerry Desktop Software functionality using the following methods:

- setting an IT policy rule to a True or False value
- typing a string, which simultaneously turns on an IT policy rule and provides the parameters for its use
- selecting a predefined permitted value to assign to an IT policy rule

Some IT policy rules have a corresponding, user-accessible field on the BlackBerry device.

- When you set an IT policy rule to a True or False value, you prevent the user from selecting another value for a corresponding field on the BlackBerry device.
- When you type a string that simultaneously turns on an IT policy rule and provides the parameters for its use, the user cannot change the value of a corresponding field on the BlackBerry device.
- When you select a predefined permitted value to assign to an IT policy rule, you restrict the values that the user can set for a corresponding field on the BlackBerry device.

You can add a standard IT policy rule to, remove a standard IT policy rule from, or change the assigned value of a standard IT policy rule in an IT policy. You cannot add, remove, or change the permitted values for a standard IT policy rule. You also cannot delete the standard IT policy rules.

You can add a new IT policy rule to, remove a new IT policy rule from, or change the assigned value of a new IT policy rule in an IT policy the same way that you change a standard IT policy rule in an IT policy.

The BlackBerry Manager groups the IT policy rules by common properties or by application. Most IT policy rules are intended to be assigned to more than one BlackBerry device. Some IT policy rules configure a unique value and are intended to be assigned to one BlackBerry device and one user only. See the *BlackBerry Enterprise Server Implementation Guide for Wireless LAN* for more information on those IT policy rules.

Reverting to the default behavior

To revert to the default behavior that an IT policy rule customizes or controls, you can set that IT policy rule to Default, if that setting is available, or delete the value that you previously set.

If you assign users to a new IT policy, you can delete that IT policy to revert those users to the default behavior for all functionality on the BlackBerry device and desktop software. The BlackBerry Enterprise Server automatically reassigns the users to the Default IT policy and resends the Default IT policy to the BlackBerry device, enforcing the default settings. You cannot delete the Default IT policy.

Creating new IT policy rules to control custom applications

Create new IT policy rules to control custom applications that your company develops to run in BlackBerry environments. After you create a new IT policy rule, you can add it to and assign a value to it in any new or existing IT policy. Only your own custom applications can use new IT policy rules that you create. You cannot create new IT policy rules to control standard BlackBerry device functionality.

Enforcing IT policy changes wirelessly

Wireless IT policy enables you to immediately enforce IT policy rule additions, deletions, or modifications on C++-enabled BlackBerry devices running BlackBerry device software version 2.5 or later and on Java-enabled BlackBerry devices running BlackBerry device software version 3.6 or later. When the BlackBerry device receives an updated Default IT policy or a new IT policy, the BlackBerry device and BlackBerry Desktop Software apply the configuration changes.

The BlackBerry Enterprise Server must resend the IT policy to the BlackBerry device to update the BlackBerry device and desktop software behavior wirelessly. By default, the BlackBerry Enterprise Server is designed to resend the IT policy to the BlackBerry devices of users that are assigned to that IT policy within a short period of time after you update the IT policy.

You can also resend an IT policy to the user account of a specific BlackBerry device manually, and you can configure the BlackBerry Enterprise Server to resend IT policies to BlackBerry devices on that specific BlackBerry Enterprise Server at a scheduled interval whether or not you have changed the IT policies.

Enforcing device and desktop security

The BlackBerry Enterprise Solution offers a user many different security settings for the BlackBerry device and BlackBerry Desktop Software. For example, you can specify one or more IT policy rules to enforce the following behaviour to meet your corporate security requirements:

- Enforce encryption
- Enforce strong encryption
- Enforce password or passphrase use
- Enforce a strong password or passphrase
- Secure Bluetooth connections
- Protect user data on the BlackBerry device
- Protect master encryption keys on the BlackBerry device
- Restrict application use on the BlackBerry device

- Restrict device resources available to third-party applications

See the *Policy Reference Guide* for more information.

Controlling BlackBerry device access to the BlackBerry Enterprise Server

Turn on the Enterprise Service Policy to control which BlackBerry devices can connect to the BlackBerry Enterprise Server. After you turn on the Enterprise Service Policy, the BlackBerry Enterprise Server still permits connections from BlackBerry devices and BlackBerry-enabled devices that you previously added to the BlackBerry Enterprise Server, but it prevents connections from newly-added BlackBerry devices by default.

Define BlackBerry device criteria in an approval list to turn on and turn off BlackBerry Enterprise Server access for BlackBerry devices. BlackBerry devices that meet the approval list criteria can complete wireless enterprise activation on that BlackBerry Enterprise Server.

You can define the following types of criteria:

- specific, permitted BlackBerry device PINs as a string
- a permitted range of BlackBerry device PINs

You can also control access based on specific manufacturers and models of BlackBerry devices. The BlackBerry Manager includes lists of permitted manufacturers and models based on the properties of BlackBerry devices already added to the BlackBerry Enterprise Server. You can uncheck items on these lists to prevent further connections from BlackBerry devices of a specific manufacturer or model.

You can permit a specific user to override the Enterprise Service Policy. If you then configure the approval list with criteria that excludes that user's BlackBerry device or BlackBerry-enabled device, the user can still connect to the BlackBerry Enterprise Server.

See the *BlackBerry Enterprise Server System Administration Guide* for more information.

Protecting Bluetooth connections on BlackBerry devices

Bluetooth® wireless technology enables Bluetooth-enabled BlackBerry devices to establish a wireless connection with devices that are within a 10-meter range. Bluetooth-enabled BlackBerry devices can connect to other Bluetooth-enabled devices such as a hands-free car kit or wireless headset.

Bluetooth profiles specify how applications on Bluetooth-enabled BlackBerry devices and on other Bluetooth devices connect and are interoperable. Bluetooth-enabled BlackBerry devices implement their Bluetooth serial port profiles to establish serial connections to Bluetooth peripherals using virtual serial ports. The Bluetooth software on the BlackBerry device accesses the serial port through the BlackBerry Software Development Kit.

You can use IT policies to simultaneously manage all Bluetooth-enabled BlackBerry devices. By default, Bluetooth-enabled BlackBerry devices that are running BlackBerry Device Software version 4.0 or later include the following security measures:

- The Bluetooth radio is turned off on the BlackBerry device.
- Users must request a connection or pairing on the BlackBerry device with another Bluetooth device. Users must also type a shared secret key (called a passkey) to complete the pairing.
- Users can specify whether to encrypt data traffic to and from the BlackBerry device over Bluetooth connections. The BlackBerry Enterprise Solution uses the passkey to generate encryption keys.
- The BlackBerry device prompts the user each time a Bluetooth device attempts to connect to the BlackBerry device.

See *Security for BlackBerry Devices with Bluetooth Wireless Technology* for more information.

Protecting the BlackBerry device against malware

Java-based BlackBerry devices are designed to provide an open platform for third-party wireless enterprise application development. Using BlackBerry MDS Studio™ and the BlackBerry Java Development Environment (JDE), the BlackBerry Enterprise Solution enables software developers to create third-party applications for BlackBerry devices. BlackBerry JDE developers can create more powerful, sophisticated applications than are possible with standard Java™ 2 Platform Micro Edition (J2ME™). A third-party BlackBerry application can perform the following tasks on the BlackBerry device:

- communicate and share persistent storage with other third-party BlackBerry applications
- interact with native BlackBerry applications
- access user data such as calendar appointments, email messages, and contacts

Third-party applications that are designed with malicious intent to cause harm to computer systems (for example, viruses, trojans, worms and spyware) are commonly known, collectively, as malware. By default, Java-based BlackBerry devices can download any third-party application wirelessly using the BlackBerry Browser. You can also send third-party applications to BlackBerry devices wirelessly, and install them on the BlackBerry devices automatically. The BlackBerry Enterprise Solution includes tools designed to enable you to control the manual or automatic installation of third-party applications and limit the access of untrusted applications to the BlackBerry device and its resources to help prevent malware attacks on the BlackBerry device.

Containing malware on the BlackBerry device

On desktop computers, malware prevention requires processes that both detect and contain malware attacks. Detection is the process of determining whether or not a program is malware. Effective malware detection requires a comprehensive and frequently-updated local database or a constant connection to a similarly qualified online database. While desktop computers might have access to these databases, current mobile devices do not have enough storage space for a malware database and cannot guarantee a constant connection to the Internet.

The BlackBerry Enterprise Solution is designed to use code signing, IT policies, and application control policies to contain malware by controlling third-party application access to the BlackBerry device resources and applications. These containment methods are designed to prevent malware that might gain access to the BlackBerry device from causing damage to the BlackBerry device, its applications and its data, or to the corporate network.

BlackBerry Enterprise Solution security method	Description
code signing	• RIM controls the use of APIs that include sensitive packages, classes, or methods to prevent unauthorized, malicious applications from accessing data on the BlackBerry device. Before you or a user can run a third-party application that uses the RIM-controlled APIs on the BlackBerry device, RIM's signing authority system must use public key cryptography to authorize and authenticate the application code. The third-party application developer must visit www.blackberry.com/developers/downloads/jde/api.shtml to register with the RIM signing authority system for access to the controlled APIs and use the BlackBerry Signature Tool that is a component of the BlackBerry JDE to request, receive, and verify a digital code signature from RIM for the application. RIM does not inspect or verify third-party applications. • Third party application developers who create controlled access third-party APIs can act as a signing authority for those APIs. The application developer can download and install the BlackBerry Signing Authority Tool to enable other developers to register for access to the application developer's controlled APIs. Registered developers can use their BlackBerry Signature Tool to request, receive, and verify digital code signatures from the application developer's BlackBerry Signing Authority Tool for their applications. Each third-party application requires authorization to run on the BlackBerry device. MIDlets (applications that use standard MIDP and CLDC APIs only) cannot write to memory on a BlackBerry device, access the memory of other applications, or access the persistent data of other MIDlets unless they are digitally signed by RIM's signing authority system. See the *BlackBerry Signing Authority Tool Administrator Guide* for more information.
using IT policy rules	The BlackBerry Enterprise Server includes IT policy rules that are designed to enable you to control third-party applications by configuring • whether or not the BlackBerry device can download third-party applications • whether or not third-party applications on the BlackBerry device can use BlackBerry device ports for communication • whether or not third-party applications on the BlackBerry device can use persistent storage on the BlackBerry device **Note**: You cannot use IT policy to permit or prevent downloading specific applications on the BlackBerry device.

BlackBerry Enterprise Solution security method	Description
using application control policy rules	The BlackBerry Enterprise Server application control policy rules are designed to enable you to permit or prevent the installation of specific third-party applications on the BlackBerry device and to limit the permissions of third-party applications that have obtained a digital signature from RIM's signing authority system, including • which resources (for example, email, phone, and BlackBerry device key store) third-party applications can access on the BlackBerry device • the types of connections that a third-party application running on the BlackBerry device can establish (for example, local connections, internal connections, and external connections,) • whether or not an application can access the user authenticator framework API, which permits the registration of drivers to provide two factor authentication to unlock the BlackBerry device For example, to permit users in your organization to use a trusted application to send and receive data from internal servers, permit the trusted application to make internal connections but prevent all other third-party applications from making internal connections. You can also set application policy rules for user groups (for example, permit an application to access internal servers for a small subset of trusted users only).

Protecting lost, stolen, or replaced BlackBerry devices

You control BlackBerry devices remotely to immediately protect confidential enterprise information using IT Admin commands.

IT Admin command	Description
Set a Password and Lock the Device	Use this command to create a new password and lock a lost BlackBerry device remotely. You can then verbally communicate the new password to the user when they locate their BlackBerry device. When the user unlocks the BlackBerry device, the BlackBerry device prompts the user to accept or reject the new password change. **Note:** If a user forgets the password for a BlackBerry device on which content protection is turned on, do not use the Set a Password and Lock the Device command to reset the password remotely. If you reset the user's password remotely, the content-protected BlackBerry device prompts the user to type the BlackBerry device password, which they have forgotten, before they type a new password because content protection uses the password to encrypt the content protection key.
Erase Data and Disable Device	Use this command to remotely erase all user information and application data that the BlackBerry device stores. You can use this command to prepare a BlackBerry device for transfer between users in your organization.

Erasing data from BlackBerry device memory and making the BlackBerry device unavailable

The BlackBerry device erases its user and application data when any of the following events occur:

- The user clicks Wipe Device (in the Security options) on the BlackBerry device.
- The user types the password incorrectly more times than the Set Maximum Password Attempts IT policy rule allows. (The default is ten attempts.)
- You send the Erase Data and Disable Device IT Admin command to the BlackBerry device from the BlackBerry Manager.

The BlackBerry device wipe process is designed to delete all data in memory and overwrite memory with zeroes. If content protection is turned on, the BlackBerry device also uses a memory scrub process to overwrite the BlackBerry device flash memory file system. The BlackBerry memory scrub process complies with United States government requirements for clearing sensitive user data, including Department of Defense directive 5220.2-M and National Institute of Standards and Technology Special Publication 800-88.

When the BlackBerry device erases its stored user and application data, it also performs the following actions:

BlackBerry device action	Description
delete the master encryption key	The BlackBerry device deletes its references to the master encryption key in memory.
unbind the IT policy	The BlackBerry device deletes the IT policy public key from its NV store so that it can receive a new IT policy and digitally signed IT policy public key from a BlackBerry Enterprise Server. The BlackBerry device does not delete its stored IT policy.
unbind the smart card (if applicable)	The BlackBerry device deletes the smart card binding information from the NV store so that a user can authenticate with the BlackBerry device using a new smart card.

See "Appendix D: BlackBerry device wipe process" on page 51 for more information.

Unbinding the smart card from the BlackBerry device

You can remove the smart card binding information from the BlackBerry device in different ways, depending on the versions of BlackBerry device software and the S/MIME Support Package that are installed on the BlackBerry device.

Software versions	Unbinding method
BlackBerry Device Software version 3.6 or earlier with either the S/MIME Support Package version 1.5 or no S/MIME Support Package installed	• Use the Smart Card Migration Tool to remove the binding between a user's current smart card and the BlackBerry device.
BlackBerry Device Software version 3.6 or earlier with the S/MIME Support Package version 4.0 or later installed; or BlackBerry Device Software version 4.0 or later (the S/MIME Support Package is optional)	• Send the Erase Data and Disable Device IT Admin command to the BlackBerry device to remove the binding between a user's current smart card and the BlackBerry device. • When you or the user disables two-factor authentication, the BlackBerry device turns off two-factor authentication with the installed smart card and deletes the smart card binding information from the BlackBerry device.

Visit www.blackberry.com/knowledgecenterpublic/ to view the article KB-03125 "How to Download and use the Smart Card Migration Tool."

Related resources

Resource	Information
BlackBerry Enterprise Server Feature and Technical Overview	• BlackBerry Enterprise Server architecture
BlackBerry Enterprise Server Installation Guide	• network environment settings • messaging and collaboration environment settings • database environment settings
BlackBerry Enterprise Server System Administration Guide	• generating and changing master encryption keys • enabling encryption • managing security
BlackBerry Enterprise Solution Security Acronym Glossary	• full terms substituted by acronyms in this and other security documents
BlackBerry Signing Authority Tool Administrator Guide	• the BlackBerry Signing Authority Tool implementation of public key cryptography • installing, setting up, and managing the BlackBerry Signing Authority Tool • restricting access to APIs
BlackBerry Java Development Environment BlackBerry Application Developer Guide Volume 1	• using BlackBerry APIs • APIs, classes, and methods with limited access • retrieving custom IT policy rules from the IT policy API • deploying applications using the BlackBerry Desktop Software • deploying applications wirelessly
BlackBerry Java Development Environment BlackBerry Application Developer Guide Volume 2	• using controlled APIs • code signatures
BlackBerry Smart Card Reader Security White Paper	• secure pairing between the BlackBerry device and the BlackBerry Smart Card Reader • initial key establishment protocol • connection key establishment protocol
Garbage Collection in the BlackBerry Java Development Environment	• cleaning BlackBerry device memory
Policy Reference Guide	• using BlackBerry Enterprise Server IT policies
PGP Support Package White Paper	• PGP security and encryption • using PGP Universal Server to store and manage PGP keys • searching for and validating PGP keys • sending and receiving PGP messages

Resource	Information
PGP Support Package User Guide Supplement	• installing the PGP Support Package • managing PGP keys on the BlackBerry device • setting PGP options for digitally signing and encrypting messages
S/MIME Support Package White Paper	• S/MIME security and encryption • managing S/MIME certificates on the BlackBerry device and desktop computer
S/MIME Support Package User Guide Supplement	• installing the S/MIME Support Package • managing certificates on the BlackBerry device and desktop computer • setting S/MIME options for digitally signing and encrypting messages • sending and receiving S/MIME messages
Security for BlackBerry Devices with Bluetooth Wireless Technology	• Bluetooth wireless technology overview • using and protecting Bluetooth-enabled BlackBerry devices • risks of using Bluetooth wireless technology on mobile devices
BlackBerry Wireless Enterprise Activation Technical Overview	• wireless enterprise activation process • wireless master encryption key generation • initial key establishment protocol • key rollover protocol
Wireless LAN Security	• security options for implementing a supported BlackBerry device on a WLAN

Appendix A: RIM Cryptographic Application Programming Interface

The RIM Crypto API on the BlackBerry device and in the BlackBerry JDE provides developers with a toolkit of cryptographic algorithms and support tools that they can use to create secure applications for business connectivity. RIM uses code signing to authorize running secure applications on the BlackBerry device and to control third-party application access to the RIM Crypto API.

The RIM Crypto API consists of a Java interface and encryption algorithm, key agreement and signature scheme, key generation protocol, message authentication, message digest, and hash code. Developers can use the JDE Java interface to access the RIM Crypto API encryption algorithms and other code to create simple solutions. Developers do not need to modify or directly access the encryption code because all calls to the native C++ encryption code are routed through the JDE Java code.

Cryptographic functionality that the RIM Crypto API provides

Symmetric block algorithms

Algorithm (uses PKCS#5 for padding)	Key length (bits)	Modes (implemented separately from the block encryption algorithms themselves)
AES	128, 192, and 256	ECB, CBC, CFB, OFB, X
DES	56	ECB, CBC, CFB, OFB, X
RC2	8 to 1024	ECB, CBC, CFB, OFB, X
RC5	0 to 2040	ECB, CBC, CFB, OFB, X
Skipjack	80	ECB, CBC, CFB, OFB, X
Triple DES	112 and 168	ECB, CBC, CFB, OFB, X
CAST5-128	128	ECB, CBC, CFB, OFB, X

Symmetric stream encryption algorithms

Algorithm	Key length (bits)
ARC4	unlimited

Asymmetric stream encryption algorithms

Algorithm	Key length (bits)
ECIES	unlimited (160 to 571 for seeding)

Asymmetric encryption algorithms

Algorithm	Key length (bits)	Type
RSA raw	512 to 4096	integer factorization
RSA with PKCS#1 formatting (version 1.5 and 2.0)	512 to 4096	integer factorization
RSA with OAEP formatting	512 to 4096	integer factorization
El Gamal	512 to 4096	discrete logarithm

Key agreement schemes

Algorithm	Key length (bits)	Type
DH	512 to 4096	discrete logarithm
KEA	1024	discrete logarithm
ECDH	160 to 571	(EC) discrete logarithm
ECMQV	160 to 571	(EC) discrete logarithm

Signature schemes

Algorithm	Key length (bits)	Type
DSA	512 to 1024	discrete logarithm
RSA using PKCS#1 (version 1.5 and 2.0)	512 to 4096	integer factorization
RSA using ANSI X9.31 **Note**: ANSI X9.31 uses one of the following algorithms for the required message digest code: SHA-1, 256, 384, or 512 or RIPEMD-160.	512 to 4096	integer factorization
RSA using PSS	512 to 4096	integer factorization
ECDSA	160 to 571	(EC) discrete logarithm
ECNR	160 to 571	(EC) discrete logarithm

Key generation

Algorithm	Key length (bits)	Type
RSA	512 to 2048	integer factorization
DH	512 to 4096	discrete logarithm
DSA	512 to 1024	discrete logarithm
EC	160 to 571	(EC) discrete logarithm

Message authentication codes

Code	Key length (bits)
CBC MAC	variable (block cipher key length)
HMAC	variable

Message digest codes

Code	Digest length (bits)
SHA-1, 224, 256, 384, 512	160, 224, 256, 384, 512
MD2	128
MD4	128
MD5	128
RIPEMD-128, 160	128, 160

Appendix B: TLS and WTLS standards that the RIM Crypto API supports

The TLS and WTLS protocol cipher suite components that the RIM Crypto API supports apply only to WTLS and handheld (direct) mode TLS/SSL on the BlackBerry device.

The RIM Crypto API implementation of the TLS and WTLS protocols supports the use of RSA and DSA public key algorithms and the DH key exchange algorithm, with the following limitations:

Cipher suite type	Typical component limitation (in bits)
export	• RSA and DH: 1024 bits or less • EC: 163 bits or less
non-export	• non-elliptic curve operations: 4096 bits • elliptic curve operations: 571 bits **Note**: These limitations are due to computational constraints on the BlackBerry device.

Key establishment algorithm cipher suites that the RIM Crypto API supports

Direct mode SSL	Direct mode TLS	WTLS
RSA_EXPORT	RSA_EXPORT	RSA_anon
DH_anon_EXPORT	DH_anon_EXPORT	RSA_anon_512
DHE_DSS_EXPORT	DHE_DSS_EXPORT	RSA_anon_768
RSA	RSA	RSA
DHE_DSS	DHE_DSS	RSA_512
DH_anon	DH_anon	RSA_768
		DH_anon
		DH_anon_512
		DH_anon_768

Symmetric algorithms that the RIM Crypto API supports

Direct mode SSL	Direct mode TLS	WTLS
RC4 40	RC4 40	RC5 40
DES 40	RC4 56	RC5 56
DES	RC4 128	RC5 64
Triple DES	DES 40	RC5
RC4 128	DES	RC5 128
	Triple DES	DES 40
	AES 128	DES
	AES 256	Triple DES
	RC4 128	

Hash algorithms that the RIM Crypto API supports

Direct mode SSL	Direct mode TLS	WTLS
MD5	MD5	SHA
SHA1	SHA1	SHA 40
		SHA 80
		MD5
		MD5 40
		MD5 80

Appendix C: Previous version of wired master encryption key generation

Each time a BlackBerry Enterprise Server or BlackBerry Desktop Software version earlier than 4.0 calls the master encryption key generation function, the C language srand function is seeded with the current time to generate a seed for the C language rand function. When the user responds to the BlackBerry Desktop Software prompt by moving the mouse, the rand function is designed to generate random data based on the entropy that the mouse movement gathers.

Previous version of wired master encryption key generation process

1. When the user moves the mouse, the BlackBerry Enterprise Server or BlackBerry Desktop Software generates either 2 or 4 bits, depending on whether one or both of the x and y axes have changed. The BlackBerry Enterprise Server or BlackBerry Desktop Software samples bits in this way until accumulating at least 8 bits.
2. The rand function generates a random integer.
3. The BlackBerry Enterprise Server or BlackBerry Desktop Software examines the integer's least significant bit. If the bit is a 1, the BlackBerry Enterprise Server or BlackBerry Desktop Software stores 1's complement of the 8 accumulated bits; otherwise, the BlackBerry Enterprise Server or BlackBerry Desktop Software stores the 8 accumulated bits unmodified. This process is designed to make sure that, even if a user replicates a previous user's mouse movements (which is virtually impossible), the resulting value is still unique.
4. The algorithm loops until the BlackBerry Enterprise Server or BlackBerry Desktop Software has sampled 256 random bits from the user's mouse movements.
5. The BlackBerry Enterprise Server or BlackBerry Desktop Software uses the SHA1 function to hash the 256 bits.
6. The BlackBerry Enterprise Server or BlackBerry Desktop Software generates the master encryption key using the first 128 bits of the resulting hash.

Appendix D: BlackBerry device wipe process

A BlackBerry device wipe is designed to delete and overwrite the BlackBerry device memory using the following process:

1. The BlackBerry device sets a Device Under Attack flag in the NV store.

   If a user removes the battery before the BlackBerry device data wipe ends, when the BlackBerry device power is restored (in other words, a user replaces the battery), the BlackBerry device wipe process continues because the Device Under Attack flag is still present.
2. If content protection of master encryption keys is turned on on the BlackBerry device, the BlackBerry device overwrites the copy of the grand master key in RAM with zeroes.
3. The BlackBerry device deletes its binding with the BlackBerry Enterprise Server by deleting the IT policy public key from the NV store.
4. If applicable, the BlackBerry device deletes the smart card binding information from the NV store.
5. The BlackBerry device radio turns off.
6. The BlackBerry device deletes data in the persistent store in flash memory, including references to the master encryption key.
7. The BlackBerry device overwrites flash memory with zeroes.
8. The BlackBerry device memory scrub process overwrites the BlackBerry device heap in RAM, changing the state of each bit four times. See "Memory scrub process for RAM" below for more information.
9. The BlackBerry device clears the BlackBerry device password from the NV store.
10. If content protection is turned on, the BlackBerry device memory scrub process overwrites the BlackBerry device flash memory file system, changing the state of each bit four times. See "Memory scrub process for flash memory" below for more information.
11. The BlackBerry device clears the Device Under Attack flag from the NV store.
12. The BlackBerry device restarts.

Memory scrub process for RAM

The BlackBerry device memory scrub process performs the following actions to overwrite the BlackBerry device heap in RAM:

1. Writes 0x33 to each byte ($0011\ 0011_2$).
2. Clears all bytes to 0x00 ($0000\ 0000_2$).
3. Writes 0xCC to each byte ($1100\ 1100_2$).
4. Clears all bytes to 0x00 ($0000\ 0000_2$).
5. Writes 0x55 to each byte ($0101\ 0101_2$).
6. Clears all bytes to 0x00 ($0000\ 0000_2$).
7. Writes 0xAA to each byte ($1010\ 1010_2$).

Memory scrub process for flash memory

If content protection is enabled, the BlackBerry device memory scrub process performs the following actions to overwrite the BlackBerry device flash memory during a BlackBerry device wipe:

1. Writes 0x33 to each byte ($0011\ 0011_2$).
2. Clears all bytes to 0xFF to each byte ($1111\ 1111_2$).

3. Writes 0xCC to each byte ($0x1100\ 1100_2$).
4. Clears all bytes to 0xFF ($1111\ 1111_2$).
5. Writes 0x55 to each byte ($0x0101\ 0101_2$).
6. Clears all bytes to 0xFF ($1111\ 1111_2$).
7. Writes 0xAA to each byte ($0x1010\ 1010_2$).
8. Clears all bytes to 0xFF ($1111\ 1111_2$).

Appendix E: Ephemeral AES encryption key derivation process

The BlackBerry device uses an ephemeral 256-bit AES encryption key to encrypt the content protection key and the ECC private key. The BlackBerry device derives the ephemeral 256-bit AES encryption key from the BlackBerry device password using the following process:

1. The BlackBerry device selects a 64-bit salt (random data to mix with the BlackBerry device password). This is intended to keep two identical passwords from turning into the same key.
2. The BlackBerry device concatenates the salt, the password, and the salt again into a byte array (Salt|Password|Salt).
3. The BlackBerry device hashes the byte array with SHA256.
4. The BlackBerry device stores the resulting hash in a byte array called a key.

   (key) = SHA256(Salt|Password|Salt)
5. The BlackBerry device hashes (key) 18 more times. It stores the result into (key) each time. For example, for i=0 to 18, the BlackBerry device does the following:

   (key) = SHA256(key)

   i++

   done
6. The final hash creates the ephemeral key.

See the *RSA Security –PKCS #5* for more information.

Part number: 7121119version2

©2006 Research In Motion Limited. All Rights Reserved. The BlackBerry and RIM families of related marks, images, and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, "Always On, Always Connected", the "envelope in motion" symbol, and BlackBerry are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

The Bluetooth word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by Research In Motion Limited is under license. IBM, Lotus, Domino, and Lotus Notes are registered trademarks of IBM in the United States and/or other countries. Microsoft, Exchange, PowerPoint, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Novell and GroupWise are either registered trademarks or trademarks of Novell, Inc., in the United States and other countries. PGP is either a registered trademark or trademark of PGP Corporation in the United States and other countries. Sun, Java, and J2ME are either registered trademarks or trademarks of Sun Microsystems, Inc. in the United States and other countries. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

The BlackBerry device and/or associated software are protected by copyright, international treaties and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in various countries around the world. Visit www.rim.com/patents.shtml for a current list of RIM [as hereinafter defined] patents.

This document is provided "as is" and Research In Motion Limited and its affiliated companies ("RIM") assume no responsibility for any typographical, technical, or other inaccuracies in this document. RIM reserves the right to periodically change information that is contained in this document; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this document to you in a timely manner or at all. RIM MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR COVENANTS, EITHER EXPRESS OR IMPLIED (INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, MERCHANTABILITY, DURABILITY, TITLE, OR RELATED TO THE PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE REFERENCED HEREIN OR PERFORMANCE OF ANY SERVICES REFERENCED HEREIN). IN CONNECTION WITH YOUR USE OF THIS DOCUMENTATION, NEITHER RIM NOR ITS RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, OR CONSULTANTS SHALL BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER BE THEY DIRECT, ECONOMIC, COMMERCIAL, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR INDIRECT DAMAGES, EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF BUSINESS REVENUE OR EARNINGS, LOST DATA, DAMAGES CAUSED BY DELAYS, LOST PROFITS, OR A FAILURE TO REALIZE EXPECTED SAVINGS.

This document might contain references to third-party sources of information, hardware or software, products or services and, or third-party web sites (collectively the "Third-Party Information"). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third-Party Information. The inclusion of Third-Party Information in this document does not imply endorsement by RIM of the Third-Party Information or the third-party in any way. Installation and use of Third-Party Information with RIM products and services may require one or more patent, trademark, or copyright licenses in order to avoid infringement of the intellectual property rights of others. Any dealings with Third-Party Information, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third-party. You are solely responsible for determining whether such third-party licenses are required and are responsible for acquiring any such licenses relating to Third-Party Information. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use Third-Party Information until all such applicable licenses have been acquired by you or on your behalf. Your use of Third-Party Information shall be governed by and subject to you agreeing to the terms of the Third-Party Information licenses. Any Third-Party Information that is provided with RIM products and services is provided "as is." RIM makes no representation, warranty, or guarantee whatsoever in relation to the Third-Party Information and RIM assumes no liability whatsoever in relation to the Third-Party Information even if RIM has been advised of the possibility of such damages or can anticipate such damages.